UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION: UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT: Approved for public release; distribution is unlimited
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION: Computer Science Dept. Naval Postgraduate School; 6b. OFFICE SYMBOL (if applicable): CS/Ln	7a. NAME OF MONITORING ORGANIZATION: Naval Postgraduate School
6c. ADDRESS (City, State, and ZIP Code): Monterey, CA 93943-5000	7b. ADDRESS (City, State, and ZIP Code): Monterey, CA 93943-5000
8a. NAME OF FUNDING/SPONSORING ORGANIZATION; 8b. OFFICE SYMBOL (if applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS: PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO

11. TITLE (Include Security Classification)

IMPROVING SECURITY IN THE FDDI PROTOCOL

12. PERSONAL AUTHOR(S)
Jones, Benjamin E.

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Master's Thesis	FROM 07/90 TO: 09/92	September 1992	73

16. SUPPLEMENTARY NOTATION: The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the United States Government.

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The arrival of high speed packet switched fiber optic LANs has allowed local area design architectures to be used for large metropolitan area network (MAN) implementations. The current LAN security mechanisms used in larger and faster fiber opti LANs and MANs are often inappropriate or unacceptable for use with emerging applications.

The protocol of the Fiber Distributed Data Interface (FDDI) standard provides a natural means for message *integrity* an *availability* verification. However, privacy in FDDI is facilitated at higher layers through a generic LAN standard. This thesi proposes a modification to the FDDI protocol implemented at the medium access control (MAC) sublayer, which integrates *confidentiality* mechanism for data transfer. The modification provides a simple comprehensive security package to meet th high performance needs of current and emerging applications.

In the proposed modification, the inherent properties of the ring are exploited using a unique Central Key Translator t distribute initial session keys. A symmetric bit stream cipher based on modulo2 addition is used for encryption/decryption b the transmitting and receiving stations. Part of the plaintext from transmitted message frames is used as feedback to generat new session keys.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION	
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	UNCLASSIFIED	
22a. NAME OF RESPONSIBLE INDIVIDUAL: G.M. Lundy	22b. TELEPHONE (Include Area Code): (408) 646-2094	22c. OFFICE SYMBOL: CS/Ln

DD FORM 1473, 84 MAR — 83 APR edition may be used until exhausted. All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

UNCLASSIFIED

Approved for public release; distribution is unlimited

IMPROVING SECURITY IN THE FDDI PROTOCOL

by

Benjamin E. Jones
Lieutenant, United States Navy
B.S., Virginia Polytechnic Institute 1983

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 1992

Author:

Department of Computer Science

ABSTRACT

The arrival of high speed packet switched fiber optic LANs has allowed local area design architectures to be used for larger metropolitan area network (MAN) implementations. The current LAN security mechanisms used in larger and faster fiber optic LANs and MANs are often inappropriate or unacceptable for use with emerging applications.

The protocol of the Fiber Distributed Data Interface (FDDI) standard provides a natural means for message *integrity* and *availability* verification. However, privacy in FDDI is facilitated at higher layers through a generic LAN standard. This thesis proposes a modification to the FDDI protocol implemented at the medium access control (MAC) sublayer, which integrates a confidentiality mechanism for data transfer. The modification provides a simple comprehensive security package to meet the high performance needs of current and emerging applications.

In the proposed modification, the inherent properties of the ring are exploited using a unique Central Key Translator to distribute initial session keys. A symmetric bit stream cipher based on modulo2 addition is used for encryption/decryption by the transmitting and receiving stations. Part of the plaintext from transmitted message frames is used as feedback to generate new session keys.

c.1

TABLE OF CONTENTS

LIST OF FIGURES

I. INTRODUCTION

A. MOTIVATION

1. Technology Trends

The continuing trend toward more advanced computer communication technologies has led to greater demands for new communication services. The use of high speed fiber optic networks has resulted in tremendous increases in data rates. One problem observed in computer network design is the lack of attention given to providing secure communications. Security controls are often applied as ad hoc mechanisms based on previous technologies or applications. In many instances a new technology may possess intrinsic properties not present in previous systems. These undeveloped properties may offer promising new methods for supporting secure communications. Likewise, the needs of new applications may make the older security mechanisms inappropriate or obsolete.

Advances in computing have resulted in more sophisticated methods of committing malicious computer network security violations. Cryptanalysis techniques have improved dramatically as a result of advances in automated data processing. Faster processors provide cryptanalysts with powerful tools for breaking ciphers. In addition, higher data rates provide the crytanalyst with more ciphertext from which encryption keys and algorithms may be discovered. The requirements and limitations associated with high speed communication technology present a dynamic situation requiring ongoing attention.

2. Recent Events

Computer Security has always been a concern among those in the industry. However recent events have focused more attention on the subject. In his book "The Cuckoo's Egg" Cliff Stoll describes his encounter with of group of West German computer hackers who successfully broke into military, government and educational computer systems using network links to U.S. computers. [Stoll 90]In 1986 a computing system at a secure scientific research laboratory in the U.S. was penetrated. In 1983 juveniles from

Milwaukee, Wisconsin, broke into many computer systems including Sloan-Kettering Hospital and Security Pacific Bank. [Pfle 89] The implications of compromised national security, invasion of financial institution records and medical facilities are enormous. Robbers can steal more with computers than with a gun; terrorists could do more permanent damage with a keyboard than with a bomb.[Adam 92] Consequently increasing attention is being focused on the shortcomings of current security systems and the need for more forethought in future system design.

3. Military Applications

a. SAFENET

The Survivable Adaptable Fiber Optic Embedded Network (SAFENET) program is part of the Next Generation Computer Resource (NGCR) program and represents the United States Navy's effort to meet the data transfer demands of Navy shipboard mission critical computer systems through development of standard computer network profiles (see Figure 1). The Navy's requirements include survivability, increased connectivity, performance and future system expansion capabilities. There are currently two SAFENET standards being developed. SAFENET-I is based on the 16 Mbps fiber media version of the IEEE 802.5 token ring architecture. SAFENET-II is based on the 100 Mbps ANSI X3T9.5 fiber distributed data interface (FDDI) protocol and is intended for Navy computer systems with high data throughput requirements. Both versions employ a graded index, radiation resistant fiber medium, with dual counter rotating rings capable of surviving five consecutive bypassed stations. Layers 3 through 7 of the International Standards Organization (ISO) are the same for both SAFENET-I and SAFENET II. System level LANs are maintained by various ships systems such as Anti-Surface Warfare (ASUW), Anti-Submarine Warfare (ASW), Hull, Machinery, Electrical (HM&E) etc. The system level LANs operate to meet the specific needs of their respective systems requirements. A backbone LAN would be used to interconnect the system LANs in order to facilitate sharing of information between systems. The system LANs would act as

concentrators to reduce the I/O requirements on the backbone. The effect of the shipwide interconnection using the backbone LAN on the basic operation of the individual systems is isolated by routers. The interconnection system allows a graceful evolution to fully distributed architectures. [Koch 91]

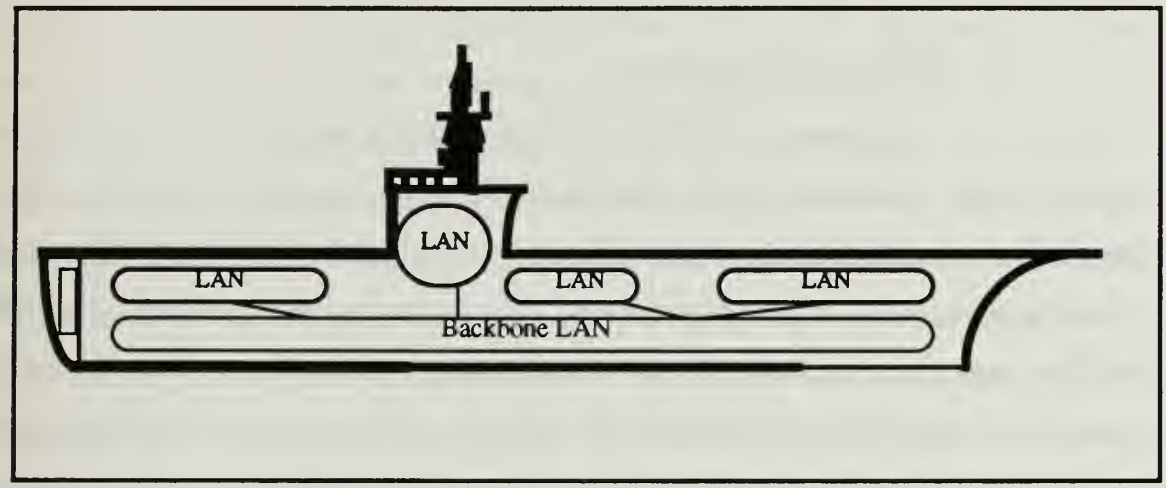

Figure 1. SAFENET Interconnect

b. Battlefield Information System

The Battlefield Information System (BIS) is the U.S. Army's future system to support the Army Tactical Command and Control System (ATCCS) in the next century. ATCSS must provide integrated network battlefield computers to support the five nodal control systems: Maneuver control, Air defense, Fire support, Combat service support and Intelligence/Electronic warfare. The ATCCS will be geographically dispersed, highly mobile and communications intensive. The current ATCCS baseline LAN consists of a coaxial Ethernet network used inside a Standard Integrated Command Post System (SICPS). The SICPS's are interconnected by a backbone single fiber optic LAN with fiber optic media access units providing a repeater function between the media. The ATCSS target system is scheduled for fielding in 1996. The anticipated replacement implementation is expected to employ Fiber Optic Tactical LAN's (FOTLAN's) within the

SICPS 's. The SICPS's in turn are interconnected by an FDDI based backbone with FDDI bridges replacing the fiber optic media access units. Additional end applications for the objective ATCSS are likely to include integrated voice, video conferencing and data graphics capabilities at single integrated workstations within distributed tactical command posts. [Hall 91]

c. Benefits and Implications

Incorporating the IEEE token ring and FDDI standards as the basis for the two SAFENET versions and the Battlefield Information Systems offers several significant advantages over current baseline systems. These benefits include added functionality, more diverse applications, and, in the case of the BIS, broader geographical coverage. The ability of the redundant ring architecture to survive and adapt when breaks occur or stations are removed is a highly desirable feature for military combat systems. The applications possibilities resulting from incorporating fiber optic communications on combat ship and battle field computer systems are almost limitless. Token ring and FDDI compatible components allow existing commercial standards to be utilized and do not require any proprietary technology. Developing LAN standards for the two SAFENET versions and the BIS diminishes the problem of nonstandard, noninteroperable networks. As a result this technology greatly enhances capabilities for high volume and high speed voice, video, data graphics and multistation video conferencing transmission. Consequently, the nature of these possible applications mandates careful attention to security controls and features which may not be available under current commercial standards.

4. Focus and Goals

The purpose of this thesis is to identify some of the positive and negative attributes associated with security of data in transfer within high speed packet switched fiber optic local area networks (FOLAN's). Specifically, we are concerned with exposing some of the inherent security enhancing qualities as well as the limitations applicable to fiber based ring architectures such as the IEEE 802.5 token ring and the ANSI FDDI

standard. The goal of this thesis is to propose modifications to the FDDI protocol that are intended to provide a simple comprehensive communications security enhancement package. The guidelines for this enhancement package are based on three basic requirements. The first requirement is that the integrity of the FDDI protocol be maintained as much as possible. Secondly, the security enhancement package should be implemented using an existing commercial encryption standard. Finally, the enhancement package complexity must be acceptable to support current applications requiring rapid response times. These restrictions are consistent with the requirements for both the SAFENET and BIS proposals. This proposed design modification is strictly intended as a foundation model for further studies in the area of high speed packet switched fiber network security. Furthermore, the proposed security modification package is not intended to replace current error checking or encryption standards but rather to provide a more comprehensive security mechanism at a lower level in the OSI model. The proposed package could be implemented as additional services and facilities at the bottom half of the data link (media access) layer. This mechanism could be used as a possible means of providing multilevel security features or it could be used as a supplemental security service in conjunction with current standards for increased privacy protection of data in transfer.

B. SCOPE

1. Security Elements

Computer network security consists of three essential elements: *confidentiality*, *integrity* and *availability*. In the context of computer security *confidentiality* means ensuring only authorized subjects may access specific objects; *integrity* means that objects can be modified only by authorized subjects (thus guaranteeing the contents of the message) and *availability* means that the objects are available to all authorized subjects. [Pfle89] In communication networks as well as computer systems, the concept of authentication is commonly used to guarantee these three elements. *Authentication* can be logically divided into *message authentication* and *peer-to-peer authentication. Message*

authentication, in the case of packet switched protocols, is concerned with verifying that the content of a message frame remains unchanged; that the message frame has not already been received and that the message frames are received in the same sequence that they were transmitted. *Peer-to-peer authentication is* concerned with verifying that a message frame actually originated from the alleged sender and that the message is successfully delivered to the intended receiver. Currently the most popular method for protecting confidentiality and integrity of data in transfer is through cryptography.[Muft 89] However, several promising non-traditional approaches to FOLAN security are emerging. These approaches are based on using properties of the physical medium or encoding schemes rather than encryption methods to support secure communications.

2. Security Threats

Security attacks against data in transfer may be passive, active, deliberate or accidental. Deliberate passive violations include unauthorized viewing of data or simply monitoring who is communicating with who. Knowing that station A is sending private data to station B can provide an intruder with much information even though the privacy of the data is protected by encryption. Deliberate active violations include unauthorized modifying of messages, withholding of messages, replaying old messages and establishing communication under another stations identity, a practice known as spurious association initiation (SAI). Accidental violations are usually cases of lost messages, accidental message modification and transmission of confidential messages in plaintext. It should be noted that although deliberate malicious attacks are the most disconcerting the majority of network security violations are caused by human error or system malfunction. [Adam 92]

The scope of this thesis is to examine LAN/MAN security with respect to the three essential elements of security. This examination is approached from the perspective of security requirements and inherent limitations of LAN's; security properties of the medium itself and security considerations specific to the token ring and FDDI protocols. The results of this examination are used to design proposed services and facilities at the Medium

Access Control (MAC) sublayer in the FDDI protocol. Encryption is currently the most popular method of providing secure communication, therefore a brief tutorial on cryptography as it applies to data in transfer is included as an appendix.

C. ORGANIZATION

This thesis is divided into four chapters plus two appendices. Chapter I has provided the purpose, scope and organization of the thesis. The second chapter examines security concerns associated with fiber optic local area networks and specifically the FDDI protocol. Some of the strengths and weaknesses associated with system design, current security mechanisms and some inherent security properties are discussed as well as several promising non-traditional methods for supporting confidential communication. Chapter III briefly describes both basic FDDI and FDDI II proceeding the discussion of the procedures used to improve security in the protocol. The concept of a key translator is introduced as a means of providing key distribution services in order to enhance confidentiality and peer-to-peer authentication capabilities. The fourth, and final chapter contains additional discussion, conclusions, recommendations and topics for future research. The first appendix contains excerpts from the X3T9.5 FDDI MAC-2 standard. The second appendix ia a brief overview on cryptography including basic data encryption methods and a discussion of several key systems used for data encryption. Appendix 2 also includes a short discussion of the Data Encryption Standard (DES), Ravist-Shamir-Adelman (RSA) encryption algorithm and a comparison of the end-to-end and link encryption methods.

II. FIBER OPTICS, LANS AND SECURITY

A. LAN/MAN ISSUES

1. LAN Issues

In terms of maintaining security, LANs possess several underlying disadvantages. The term LAN implies that the network only covers a small geographic distance such as a building, floor of a building or a campus. Local area networks are typically employed in low security environments such as educational institutions or unclassified administrative and business office applications. Consequently, LAN users are often less cognizant of security threats and policies. However, there is no maximum distance which is used to distinguish the local area network from the "larger" metropolitan area networks (MANs) and Wide Area Networks (WANs). The LAN environment was originally intended to be one of trust between professionals in non-computing fields. However, when we consider that LAN architectures are sometimes used for MAN implementations and that LANs and MANSs are often connected to other LANs and MANs and to the world via WANs, (see Figure 2) it becomes obvious that the so called "environment of trust" is not really valid. An environment based on trust is quickly weakened when users are no longer aware of who may have access to their system.

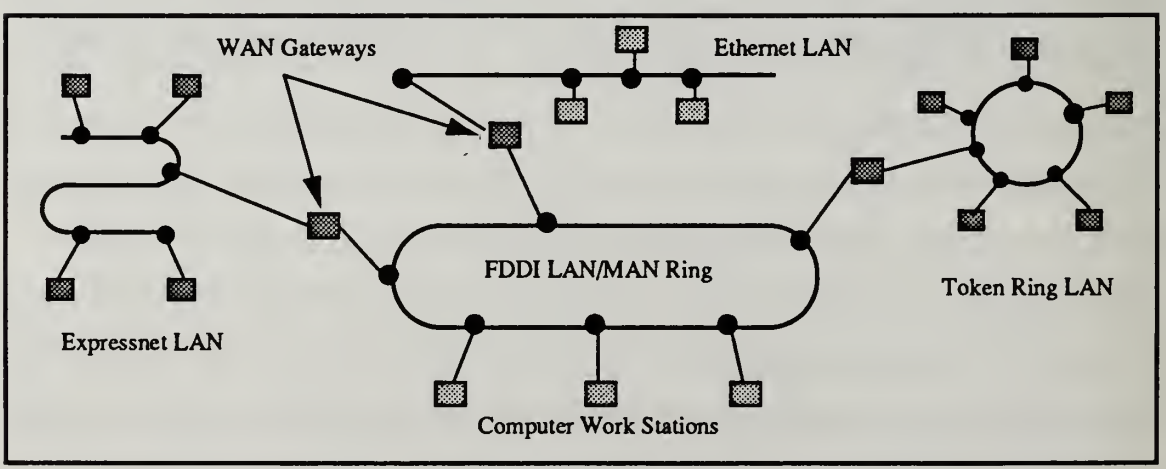

Figure 2. Interconnected Network System

Another consideration is that complex security devices used for highly classified information may not be appropriate for the average LAN. The value of the data on these networks may not warrant the added time complexity or monetary cost required of these security devices, and consequently may make them an unacceptable solution. This is a particular concern when we consider the electro-optic bottleneck problem caused by the mismatch in speeds of the high speed fiber optic medium and slower electronic components.

Security devices need to better accommodate the needs of the user application and network design in order to keep up with changes in the industry. Currently the IEEE 802 standard employs the same security mechanism for all LANS sharing the same ISO layers 3-7. [Stal 91] When the fundamental differences between the LANs which fall into this category are considered,the need for more forethought in security design becomes apparent.

Most LANs employ contention media access protocols which pose additional security problems. In contention access systems, each transmission is "broadcast" on the medium resulting in every party on the network having the potential to view all data in transfer. Additionally, authentication of stations and messages is traditionally of lesser concern in broadcast local area networks. LAN stations or nodes often represent single users who are generally authenticated during login through passwords. In passive contention designs, the "broadcast and capture" message protocol precludes any effective challenge of message authenticity. Active contention LAN's such as token ring and FDDI pose some different problems which will be discussed later in this paper.

2. Traffic Analysis

LAN's are highly susceptible to traffic analysis despite the fact that the message contents may be protected by encryption. This is because the source and destination addresses usually remain unprotected and readable by all stations. With each station typically representing a single user, the passive intruder may acquire valuable information

by determining which users are communicating with one another. An obvious example might be the problems encountered by the military trying to plan a surprise offensive. The large volume of traffic to particular locations would likely indicate to the enemy that something substantial is about to happen.

The two most common methods used to deter traffic analysis are to control the routing of messages and to pad traffic by generating spurious messages for all possible pairs of hosts. [Pfle 89] The "broadcast and capture" protocols of most local area networks make the routing control method impractical for these systems, since all messages are available to all stations on the net anyway. The message padding method implies a higher bandwidth utilization which, in the case of passive contention protocols may reduce throughput by potentially causing more collisions.

B. FIBER AND SECURITY

1. Electromagnetic vs. Light Energy

As electric current (possibly in the form of a digital signal) travels through wire or cable a magnetic field is generated. Sophisticated electronic circuitry which is not even in contact with (but in relatively close proximity to) the cable can be used to detect electromagnetic emanations. The implications of these vulnerable emanations constitutes a security threat. Additionally, copper wire and cable can easily be cut and spliced to facilitate simple active wiretaps. Active wire taps not only allow intruders to listen but also permit them to inject signals into the communication medium. [Pfle 89]

Optical fiber offers several distinct security advantages. Principally, the signal in fiber is in the form of light rather than electromagnetic (EM) energy, consequently there is no electromagnetic field which, in turn, means the signals are insensitive to electromagnetic interference and are virtually impossible to tap inductively. Additionally, the entire optical network must be carefully tuned each time a new connection is made. This makes it difficult to make a physical tap without detection. Optical fiber with intruder detection shieldings are available such as the U.S. National Security Agency (NSA) approved step

index system and bimodal graded index fibers. Both of these alarm fiber systems are transparent to the user and have self testing capabilities. [Coom 91]

2. Power and Code Division

Several other potential methods for supporting confidential communication are being studied. One non traditional way to dissuade optical tapping is through power division. This concept has been applied to the modified star configuration where the star coupler divides incoming power among all ports other than itself (see Figure 3). This is accomplished by interconnecting *N* bidirectional tree couplers such that an entering signal traverses two tree couplers in cascade resulting in a power loss of $1/(N-1)^2$. This controlled loss could be used to ensure that transmission power at all possible access points is too low to be detected by any covert couplers.[Coom 91] This method appears applicable to double tree configurations as well.

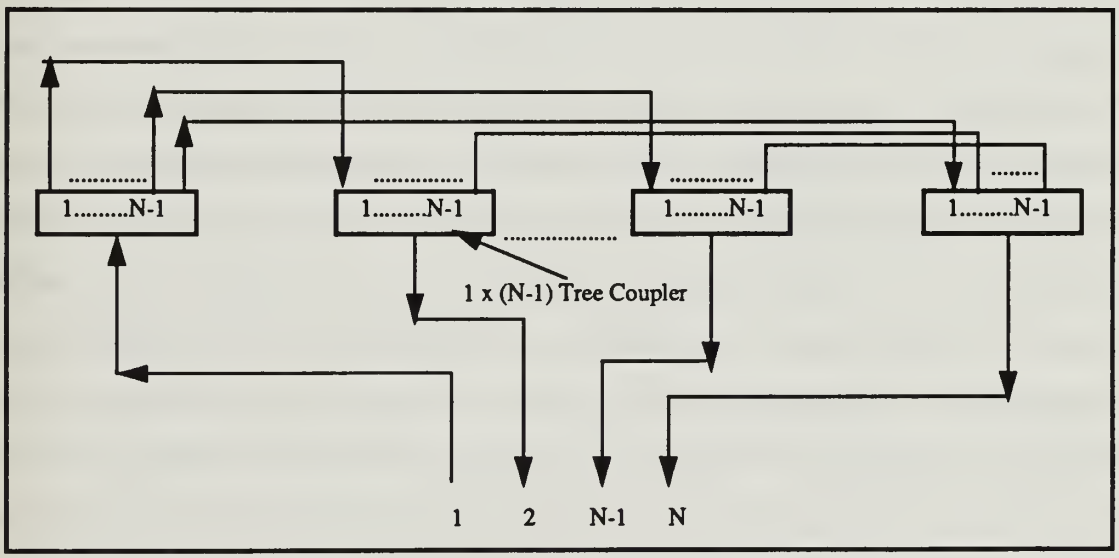

Figure 3. Schematic of Modified Star Coupler

Code Division Multiple Access (CDMA) research is another promising area with the potential to support confidential communication in fiber optic broadcast networks.

CDMA could be used as a replacement for, or a supplement to current data encryption methods as a means of providing private communications. This method involves time-multiplexing messages by transforming each pulse from a transmitter into a train of secondary pulses by suitable coding means. Only those receivers with matched decoders are therefore able to recognize the correct pulse sequences. [Marh 89]

Both of these methods are still being investigated to determine their validity and feasibility. Consequently, commercial application using CDMA and power division as a basis for maintaining communication security are probably still several years away. However, as concerns surrounding the effectiveness of data encryption continue to surface, these non traditional methods will likely gain more attention.

3. Optical Bidirectionality

Optical fiber also possesses the property of *optical bidirectionality* (OB) which is the capability of simultaneous transmission in opposite directions on the same channel without collision. The idea of using this physical characteristic as means of generating a jamming signal transmitted to unintended stations has been suggested as a means of providing a (non-conventional) privacy mechanism for passive broadcast FOLANs. The OB method is not susceptible to cryptanalysis because the signal received at each station is not ciphertext, but rather a superimposition of the jamming signal over the plaintext. However, authentication is still facilitated through encryption and is thus subject to cryptanalysis. This concept has been applied in theory to a wide variety of demand assignment multiple access (DAMA) schemes using linear buses, binary trees and modified star configurations while still maintaining the significant features of the access protocol. This method is not really practical for the token ring or FDDI protocols. Since the most obvious problems stem from the active contention access scheme and unidirectional message passing at each station. Passing along a superimposed signal to the receiving station with no way to reproduce the plaintext would be of little use. Overcoming this problem would necessitate many modifications to the physical layer in terms retrofitting of

optical couplers. In addition, major modifications would be required at the media access control (MAC) sublayer to the clocking synchronization scheme in order to facilitate confidential call set up and termination. [Marh91]

C. TOKEN RING ARCHITECTURE

In the token ring architecture it is possible for one node to deny service to another node or to compromise integrity by either withholding a message or by modifying a message before retransmitting to the next node. This is unlike typical broadcast networks employing a bus architecture where each node must capture a message as it goes by. From this perspective the security requirements of the token ring more closely resemble those of many wide area networks. In the token ring architecture there is no provision to analyze traffic flow. This means covert channels may go undetected and the authenticity of nodes is not verified. The ring architecture possesses several intrinsic security advantages not seen in other LAN architectures. The most obvious advantage is a known path between every transmit/receive station pair. Every packet (message) must pass through every other station on the ring and always terminates back at the transmitting station. This enables the transmitting station to monitor the message after it has traveled through all stations and thus check the integrity and availability of the message. The current FDDI standard incorporates a Frame Check Sequence (FCS) using cyclic redundancy checks. [FDDI 91] The purpose of the FCS is to permit the receiving station to determine whether the received message is the same as the transmitted message. In this way the message can be checked for integrity by both the receiving and transmitting stations. Figure 4 depicts a sample frame traversing a ring with an error introduced as it passes through a station along its path. A simple modulo 2 addition operation applied between the message before transmission and the returning message reveals the number and location of errors.

Although node authenticity is not verified in the ring architecture each node does monitor all traffic, comparing source addresses of passing frames with its own address. This allows originating stations to remove messages after they have traveled the entire ring

as well as detect another station pretending to be the originating station. Passing frames with matching source addresses which were not transmitted by that station signal that a possible SAI has been attempted.

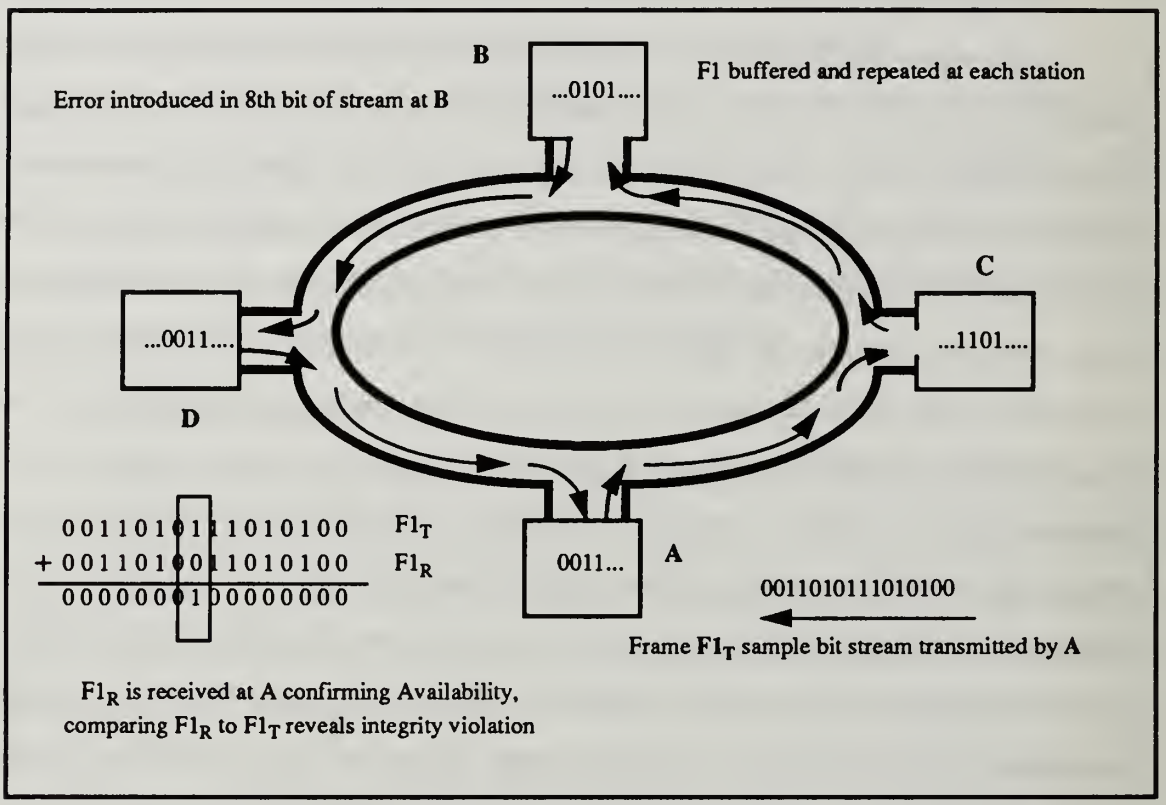

Figure 4. Token Ring Security Properties

Three potential situations which could result in disruption of service and denial of data availability are: when a station retains the token beyond its allocation, removes the token from the ring altogether or more than one token is traversing the ring at a time. In order to manage the situations of a persistently busy token, a lost (or stolen) token or multiple tokens, one station is designated as the active token monitor. The active monitor detects lost tokens by using a timeout greater than the time necessary for the longest frame to travel the entire ring. When the monitor detects a lost token the ring is purged of any residual data and a new free token is released. A persistently busy token is reset to free once

detected by the active monitor. Other stations on the ring have the role of passive monitor. Passive monitors must be able to detect active monitor failure and assume that role. A contention- resolution algorithm is used to decide which passive monitor station takes over in the event of active monitor failure. [Stal 91]

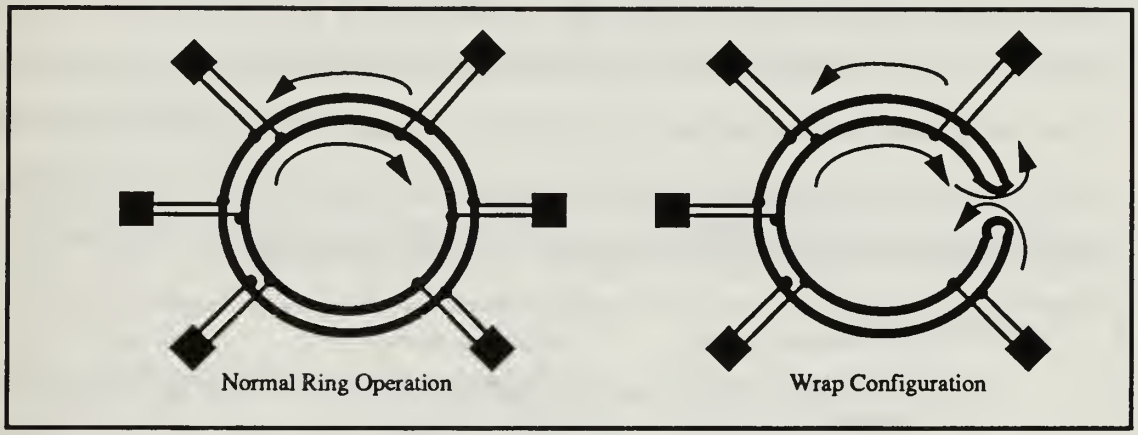

Figure 5. Dual Ring Adaptability

Another design feature of some ring architectures such as FDDI helps to alleviate the problem of multiple points of failure within the network through the use of dual counter rotating trunk rings. When a node or link fails the two counter rotating paths wrap together around the fault thus allowing continued communication. Figure 5 depicts the dual ring in the normal configuration as well as the wrap mode. This ability to adapt to breaks or node failures helps ensure reliability of the system and availability of data in transfer. [Ross 89]

III. FDDI AND SECURITY

A. FDDI

The Fiber Distributed Data Interface (FDDI) is a 100 megabit per second (Mbps) LAN using an optical fiber transmission medium. The stations are configured using two counter rotating trunk rings which permits reconfiguration of the ring in the event of failures. A total of 1000 physical connections (500 stations) and a fiber path of 200 kilometers has been used as the basis for calculation of recovery timer default values. Some of the potential services offered by FDDI include I/O channel (back-end), LAN backbone, front end high performance LAN, and circuit switched applications.

1. Basic FDDI

In Basic FDDI, a "free" token is passed from station to station to signify the ring is available for transmission of information on the next frame. If a station wants to transmit, it removes the free token from the ring. After the captured token is received, the station begins transmitting its eligible queued frames. Each frame starts with a preamble which is at least 64 bits long. The preamble is followed by an 8 bit starting delimiter, an 8 bit frame control, a 16 or 48 bit destination address and a 16 or 48 bit source address. The length of the information field is variable, but is limited by the maximum frame length of 4500 octets. The information field is followed by a 32 bit frame check sequence, 4 bit end delimiter and a frame status field. Figure 6 shows the format for an FDDI frame. Immediately after transmitting a frame the station releases the token. This allows frames from multiple stations to simultaneously propagate around the ring. [Ross 89]

Ring operation consists of each station receiving frames from its upstream neighbor station and transmitting (repeating) the frame to the next station downstream (see Figure 7). As a frame passes through a station, that stations MAC modifies indicator symbols in the Frame Status (FS) field of the frame to indicate detection of any errors in the frame. During the receive and retransmit operation, destination addresses of passing frames are compared to the MAC's address. Matching frames are copied into a local buffer at the

receiving station. Before repeating a frame, the receiving station sets indicator symbols within the FS field of the frame to inform the transmitting station of any detected errors and that the message was copied by the receiving station. A transmitted frame continues around the ring passing through connected stations until it returns to the originating station. The originating station may examine the FS field indicator symbols in the frame to determine whether the transmission was successful. The MAC of each station is responsible for recognizing returning frame Source Address (SA) fields and removing these frames from the ring. [FDDI 87]

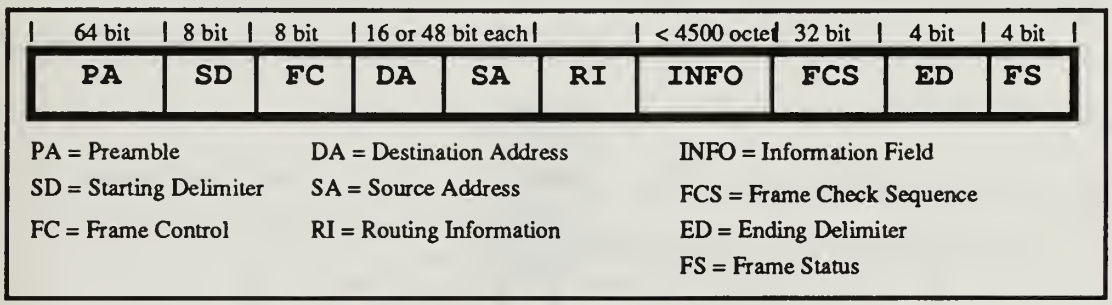

Figure 6. FDDI Frame

FDDI supports two types of traffic called *synchronous* and *asynchronous*. Synchronous service is designed for applications with predictable bandwidth and critical response times. Asynchronous services are designed for applications with bursty, widely varying bandwidth requirements. [FDDI 91]

In order to regulate synchronous traffic, station management allocates each station a fixed synchronous bandwidth. Interoperability between all stations may be maintained without synchronous transmission support at each station. This means that stations with a zero synchronous bandwidth allocation only support asynchronous transmission service. For stations capable of synchronous service, synchronous frames may be transmitted whenever the station captures a token. The station may transmit synchronous frames until the Station Allocation (SA_i) is reached. [Stal 91]

To accommodate asynchronous traffic a Target Token Rotation Time (TTRT) (negotiated during ring initialization) is defined, with each station maintaining the same value for TTRT. Each stations Token Rotation Timer (TRT) is initialized to TTRT when enabled. The TRT counts down until TRT = 0, and is then reset to TTRT again. Late Count (LC) is initialized to LC = 0 and increments each time TRT expires at TRT = 0. The Late Counter records the number of times TRT has expired since the token was last received. If TRT has not expired the token is considered to have arrived early. When a station receives the token early it may transmit asynchronous frames (after any synchronous frames have been transmitted) for a period not to exceed the remaining TRT. Once the allowed asynchronous frames have been transmitted, the token is released and the TRT and LC are reset. [FDDI 91]

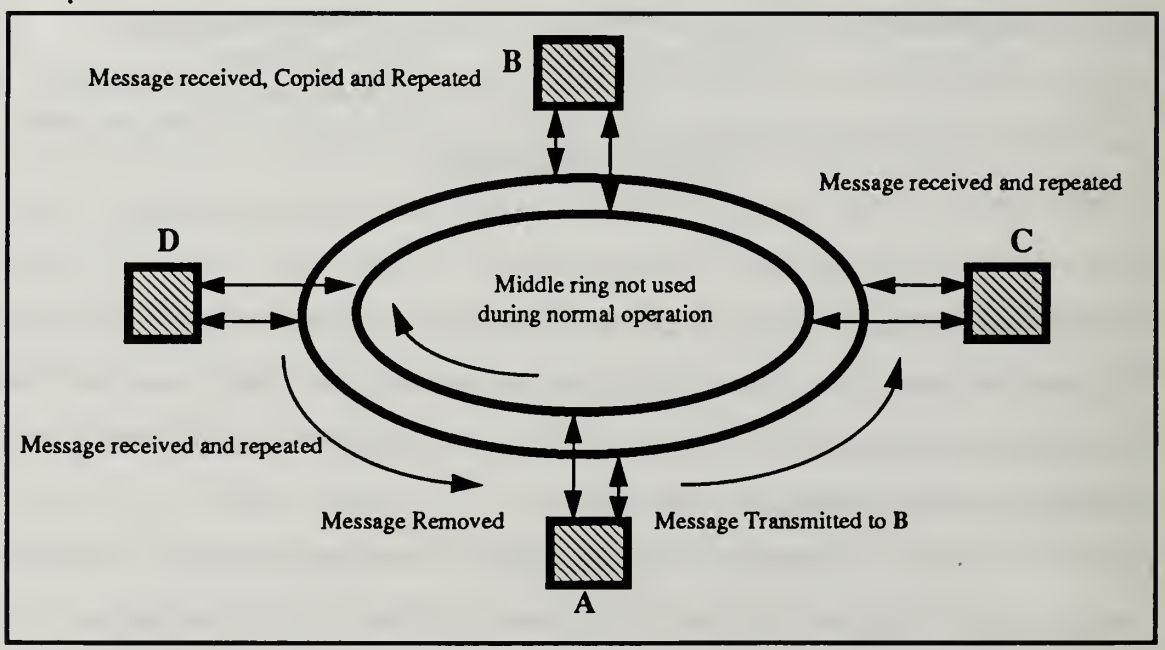

Figure 7. Fiber Distributed Data Interface

The medium access control monitoring functions are distributed among all stations on a ring. Stations continuously monitor the ring for inactivity or incorrect activity on the ring. Ring inactivity is the condition where no token is circulating. This situation is

remedied by purging the ring of all residual traffic and releasing a new free token. Incorrect ring activity is typically the result of successive expirations of the Target Rotation Timer and Late Counter. The persistently busy token, once detected, is simply reset to a free token by a monitor station.

Station Management (SMT) at each MAC, monitors ring activity and exercises control over station activity during ring operation. In the event that SMT detects a failed station, the network is reconfigured at either end of the faulty link. This removes the node from the network and allows continued operation of the ring. [Ross 89] The process of removing a faulty link is called wrapping and is depicted below in Figure 8.

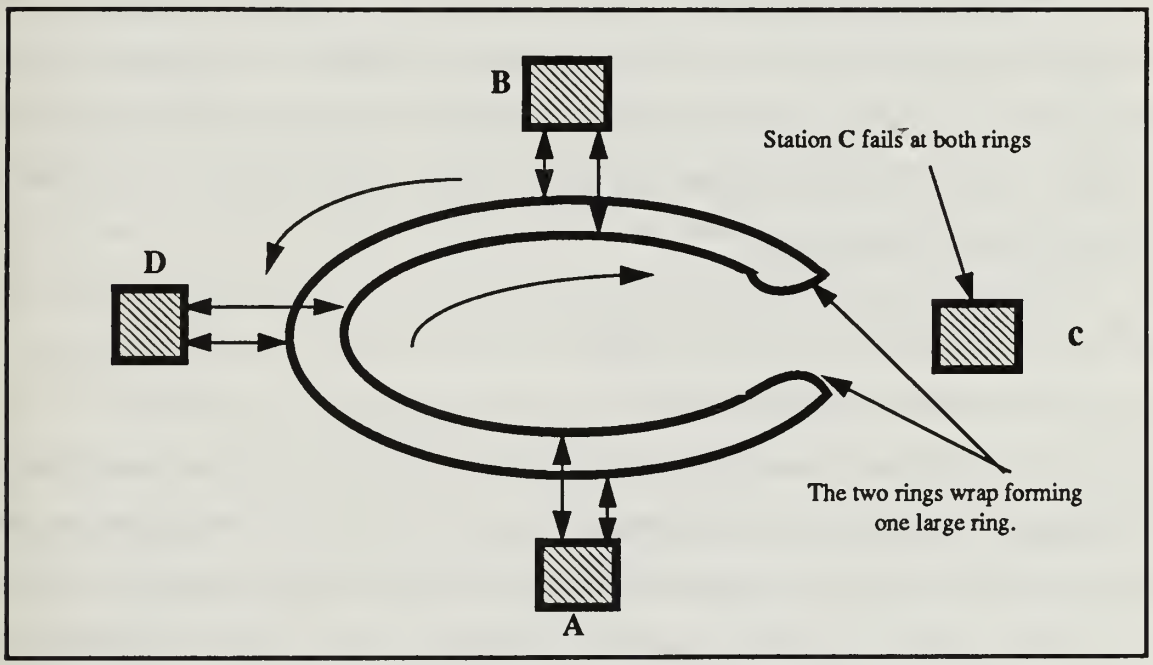

Figure 8. FDDI in the Wrap Mode

2. FDDI-II

FDDI-II is an upward compatible enhancement of basic FDDI, which includes a circuit switching capability called isochronous transmission. The primary difference between basic FDDI and FDDI-II is the addition of a hybrid mode of operation specified in the Hybrid Ring Control (HRC) document. HRC provides multiplexing of packet and circuit switched data on a shared FDDI medium. FDDI-II permits stations to operate in

either Basic Mode or in Hybrid Mode. The Hybrid Mode differs from the Basic Mode in that portions of the available bandwidth may be dynamically partitioned for circuit switched data in units of full duplex Wideband Channels (WBCs). WBCs provide a bandwidth division mechanism between the packet (synchronous and asynchronous) switched traffic and circuit (isochronous) switched traffic. Up to 16 WBCs may be assigned with each allocated up to 6.144 Mbps. The aggregate of any or all allocated WBCs may be used as one virtual service to satisfy the needs of applications with large bandwidth requirements such as high resolution video. [Ross 89] Using the 'hybrid' mode, data can be multiplexed between the packet MAC and the isochronous MAC (I-MAC). The transceiver, cable and connector systems are identical between FDDI and FDDI-II. With some of the bandwidth in the FDDI-II ring possibly allocated to isochronous services provided by the WBCs, additional services requiring virtual circuit switched services not found in basic FDDI are possible. The most obvious services include video, voice and control or sensor data streams.

B. CONFIDENTIALITY AND FDDI

1. Modification Design Issues

In Chapter I the implementation restrictions dictating the use of existing commercial encryption standards to meet the needs of current high speed applications were discussed. In addition, the proposed modification was supposed to maintain the integrity of the FDDI protocol as much as possible. Consequently, some of these restrictions were critical factors in several of the design decisions for the proposed protocol modification.

The FDDI standard is becoming much more established with networks already in use. Any proposed modification decision must be tempered with the understanding that the effect on existing systems and applications must be minimized in order for the modification to be considered viable. Substantial changes to a protocol can easily result in a cascading effect where the original protocol becomes barely recognizable. Our proposed modification is at the MAC sublayer of the FDDI protocol. The changes to the protocol

entail the addition of several procedures for encrypting and decrypting data packets. The use of these procedures results in an additional machine state for both the MAC transmitter and receiver. In addition, some additional hardware would be required to perform the high speed encryption and secure storage of keys. Additionally, one node on the ring must be dedicated to key distribution services and is required to be a trusted facility. However, the basic timing, fault management and frame management protocols have essentially remained unchanged.

Public key encryption systems have been shown to be at least as secure and often more memory efficient than private key systems for many types of applications. However, several factors surrounding public key encryption led to the decision to use a private session key mechanism and a modified conventional key server for key distribution. One of the design restriction is that any modification be consistent with the speed and bandwidth requirements associated with current and near future applications. Some of these applications will include high resolution video conferencing, circuit switched voice and data graphics capabilities. The rapid response time and large bandwidth requirements of these applications make a public key system inappropriate for encryption of data packets used in confidential communication. Public key systems require a double encryption/ decryption to provide both peer-to-peer authentication and secrecy. [Pfle 89] The double encryption constraint coupled with the speed complexity of the ciphers (see Appendix 2) make the response time of public keys unacceptable for many of the potential applications to be used.

A public key distribution mechanism could be used to distribute private session keys possibly more securely and as efficiently as a private key distribution system. However, with the exception of the Rivest-Shamir-Adelman (RSA) encryption, the public key algorithms seen to date have been shown to exhibit substantial weaknesses (see Appendix 2). [Pfle 89] This is where we must consider the design restriction to use existing commercial encryption standards. Unfortunately, the RSA encryption algorithm is not a commercial standard but rather proprietary in nature. In addition to violating one of our

basic design restrictions, the use of a proprietary system in our design would necessitate paying royalties to the patent holder.

For the reasons just presented our proposed modification is based on the use of a conventional key system such as the Data Encryption Standard (DES). The DES is a readily available commercial standard developed for government use and has undergone extensive study and testing. Although we are not endorsing the DES, it represents the model encryption standard for our proposed modification. In order to meet the needs of real time applications we shall pay particular attention to the stream cipher mode of the DES.

2. MAC Level Implementation

As explained earlier, the FDDI protocol possesses many characteristics naturally conducive to supporting secure communications. The token ring protocol provides the added message integrity and availability through fault management, error checking and station management. However, confidentiality services in FDDI are not provided as part of the FDDI protocol. In fact, privacy mechanisms for most LANs are traditionally facilitated through encryption at the Logical Link Control (LLC) sublayer or higher layers in the ISO model (see Figure 9). [Tard 85]One problem with this approach is that the same LLC is used for a variety of LAN architectures including Carrier Sense Multiple Access/Collision Detection (CSMA/CD), token bus, token ring, FDDI and several others. Performing encryption at this level does not exploit the specific characteristics of the protocol or topology. Several of the oldest most established LAN standards employ a passive contention "broadcast and capture" protocol. The "receive and forward" design of the token ring more closely resembles the point-to-point characteristics seen in many wide area networks. Using the same confidential communication system for such different systems seems grossly inappropriate.

In addition to the points just discussed, it should be mentioned that address recognition is facilitated at the MAC sublayer. Therefore, the Source Address and Destination Address of the private frame can never be encrypted at the LLC sublayer which

would help deter traffic analysis (see Figure 10). Finally, the security protection mechanisms for FDDI are scattered throughout different layers of the ISO model making them less comprehensive and less efficient.

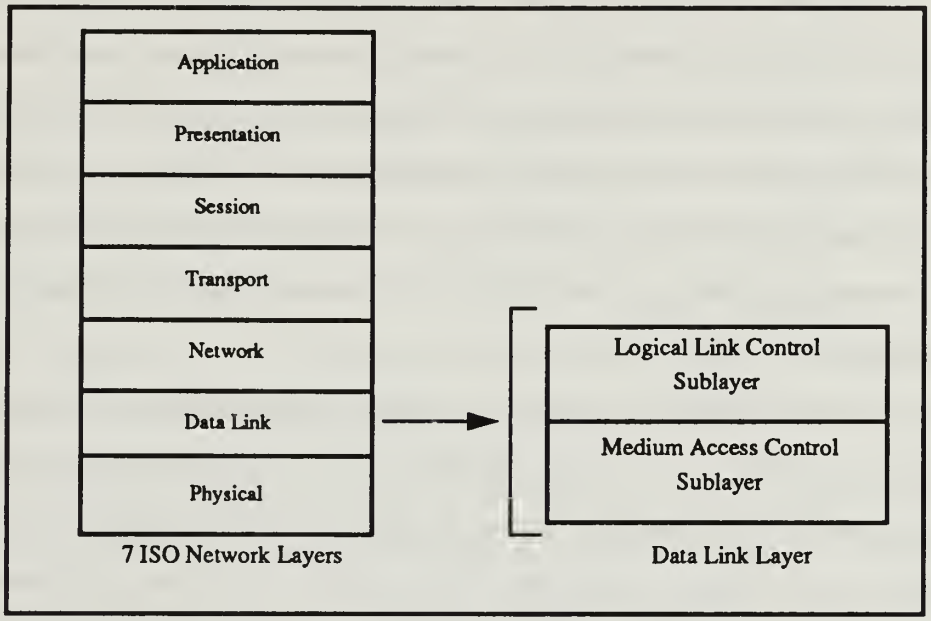

Figure 9. ISO Network Layers

We propose incorporating a simple confidential communication enhancing service implemented at the Medium Access Control (MAC) sublayer of the data link layer (see Figure 9). The service uses data encryption methods with conventional secret keys distributed through a trusted key distribution station. The actual encryption scheme would employ a type of bit stream cipher with plaintext feedback (see Appendix B section 1) such as the stream cipher mode of the DES. The bitwise cipher method was chosen because stream ciphers are relatively easy to perform, are substantially faster than block or exponential ciphers, do not propagate errors and have a linear translation complexity. The stream cipher method is particularly attractive for real time applications with voice, video and graphics requirements. Several standards using bitwise ciphers are currently available and could easily be implemented in this proposed modification. Detailed discussion of the

standard best suited for this implementation is beyond the scope of this discussion. However, a simple bit stream cipher such as the DES in the stream cipher mode could be used and is used as the model for developing our proposed method.

There are several advantages to encrypting at the MAC as opposed to the LLC sublayer. With MAC level encryption it is possible to encrypt the source address (SA) and destination address (DA) to help deter traffic analysis. Encrypting above the MAC sublayer will prevent SA and DA encryption. In addition, we can preserve the error checking capability by applying the Frame Check Sequence after the encryption has been performed on the frame. Encryption applied below the MAC sublayer would upset the Frame Check Sequence protocol.

Encrypting SA and DA addresses would require a complex address recognition function in the MAC at each station to distinguish and recognize plaintext and ciphertext SA and DA fields. The method used to encrypt these two fields must ensure that neither the ciphertext SA or DA will be a duplicate of another stations plaintext or ciphertext address. For our implementation we will express the encryption of the SA and DA fields as an optional procedure and will not go into the details of the ciphertext address recognition function.

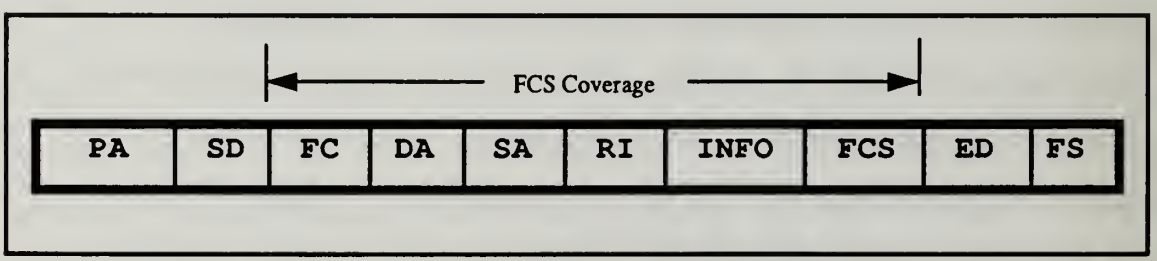

Figure 10. Frame Check Sequence Coverage in an FDDI Frame

3. Key Management

The initial key values for the stream cipher are distributed using a trusted key management scheme similar to the Erhsam method designed for the Data Encryption

Standard (see Appendix B section 3). [Ehrs 78] As discussed earlier, this is one possible alternative to using a public key distribution system. This unique variation is based on a secure node called the Central Key Translator (CKT). A key generator is used by the transmitting station **A** to generate a unique 64 bit initialization value called K_{IV}. A 64 bit value was chosen primarily because that is the length used in the DES. However, an encryption method using a different length key could be implemented for use with some other encryption standard as long as it did not exceed the maximum frame length for FDDI (4500 octets). The initial key value is encrypted using the master key Kt_A shared only by the transmitting station A and the Central Key Translator (CKT). Upon receiving the encrypted IV_{AB} value, the CKT decrypts the frame using master key Kt_A and then re-encrypts on the same frame using master key Kt_B of the receiving station **B**. The translated key is then forwarded to Station **B** which uses the master key Kt_B to decrypt the translated initial key K_{IV} value originally generated by **A**. Station **B** copies the flagged frame, generates a session key value by invoking a GENERATE_KEY procedure involving a Pseudo Random Number Generator (PRG). At the same time **B** decrypts the frame (containing initial key value) just received from the CKT. Station **B** then uses the received initial key K_{IV} (generated by A) to encrypt the session key it just generated. B's new key is then forwarded on to **A** encrypted under a key only stations A, B and the CKT share. Station **A** recognizes the returning frame and removes it from the ring. The frame is decrypted by **A** using the initial key K_{IV} (which **A** generated). Both stations **A** and **B** now share the same session key and may conduct confidential communication. Since the frame is removed by station **A** even the CKT does not posses the session key. The session keys were distributed with one traversal of the ring. The other situation is when the receiving station is logically positioned before the CKT. In this case key establishment would require two ring traversals. On the average the two station positioning situations will each occur 50% of the time resulting in an average of 1.5 ring traversals for key establishment. This is still one half the number of frame transmissions required for key establishment using the

conventional key server described in Appendix 2. The protocol for the Central Key Translator operation is depicted graphically in Figure 11.

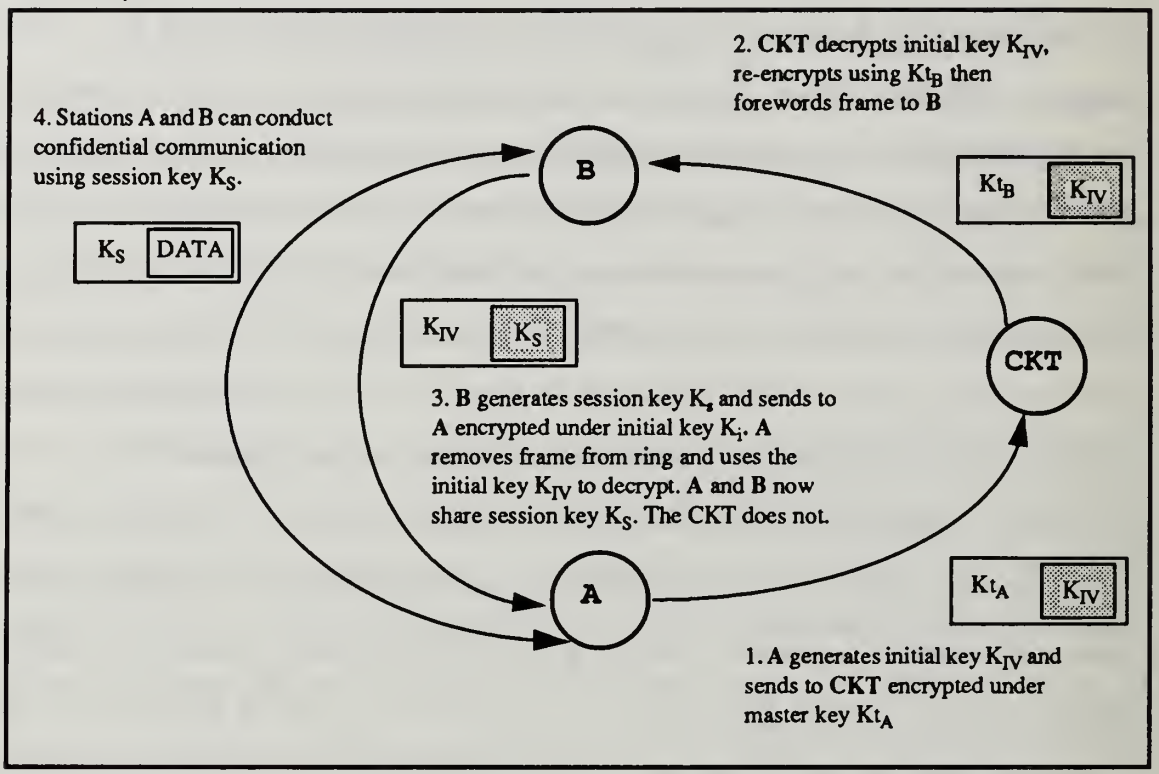

Figure 11. Central Key Translator Protocol

4. IV Buffers

Once session keys are established between two stations, they are maintained in Initial Value (IV) buffers. Each station would be capable of maintaining an individual IV buffer for every other station. This means that each station could potentially need to maintain 500 IV values since a ring may have up to 500 stations (1000 connections). However, all stations may not be capable of confidential communication or may not require confidential communication services with every station on the ring. In this case it would be possible to maintain a fixed number of IV buffers consistent with the number of stations with which a station regularly communicates confidentially (see Figure 120). To accomplish this, an procedure similar to a page replacement algorithm such as Least

Frequently Used (LFU) or Last Recently Used (LRU) could be implemented to manage which buffers would be overwritten when a particular IV_{AB} did not exist. Any station overwriting an existing key value must notify the station sharing the overwritten key that it is no longer valid. Otherwise, a transmitting station may send data frames encrypted using a key which the receiving station is no longer maintaining. By maintaining key values for station pairs we reduce the requirement for establishing a new session key each time a private communication is initiated. This is a fundamental requirement for use with rapid response time applications. The added secure memory requirement for maintaining session keys is the trade-off for this speed improvement.

In order to prevent a session key from becoming "stale" the key is changed after each received frame or series of received frames based on a pre-negotiated frame interval established between the transmitting and receiving stations. This session key generation is accomplished by using part of the plaintext from one of the INFO frames (previously negotiated) as a seed used for generating a new session key. Both the transmitting and receiving stations may generate the session key independently (without the CKT) provided the receiving station copies an error free message. In the event that an error is introduced in the frame intended to be used for key generation, both stations will be able to detect the error(s) and the previous key can be used one more time or the CKT can be used to reset the keys. The error stricken message may then be retransmitted using the same or different keys depending on the protocol. By generating a new key with each received frame or series of received frames, each key serves as a short term cipher. Periodically, the keys should be reset using the CKT even when a valid IV exists between two stations. Since all stations possessing the same key seed are capable of generating the same key it is imperative that a limited amount of cipher text under the same key be provided any cryptanalytic intruders. Consequently, only by maintaining the secrecy of the keys can we more assuredly guard the secrecy of the messages.

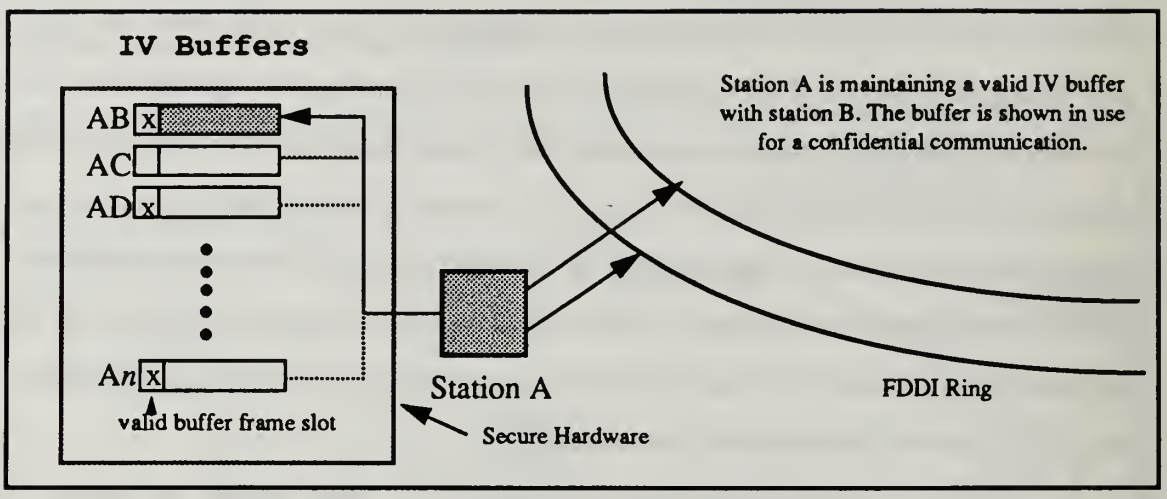

Figure 12. Station IV Buffer Management

5. Confidential Communications

When station **A** wishes to communicate confidentially with station **B**, **A** must determine if a valid IV_{AB} buffer is maintained at both stations. If the buffer is not valid **A** must initiate a RESET_KEY operation through the CKT. Assuming the buffer is valid, station **A** uses the buffer value as the key for the bit stream cipher applied to the frame(s) to be transmitted. The encryption is applied prior to setting the FCS bits. This allows the error checking facility within the fault management portion of the SMT to be maintained. Once the message is encrypted it is transmitted onto the fiber medium. The transmitted packet and IV buffer are stored until the packet has traversed the ring and returns to the originating station **A**. When the packet returns **A** checks for any errors. If no errors are detected station **A** checks the session key replacement counter. If the key replacement counter has not expired then the session key is still valid and the counter is decremented. If the counter has expired, then a portion (64 bits if using DES) of the plaintext from the previous frame is used as a seed for generation of a new A/B session key and the session key counter is reset.

When the confidential message reaches the receiving station **B**, if no errors are detected it sets the proper indicator symbols in the Frame Status field and retransmits the frame. Station **B**'s MAC then applies the bit stream cipher to the ciphertext frame just received using the value stored in the IV buffer as the session key. If the session key counter has expired, a portion of the resultant plaintext message (64 bits if using DES) is used as the seed for generating a new session key, the new key is copied into **B**'s IV_{AB} buffer and the session key counter is reset. If the session key counter has not expired, then the session key remains valid and the key counter is decremented. If errors are detected, the proper FS field indicator symbols are set, the frame is retransmitted to the next station and the current session key is maintained as valid. The confidential frame may be retransmitted under the current session or may be encrypted under a new session key following a RESET_KEY operation.

6. Security Procedures

a. CALL_SETUP

The call set up is initiated when station **A** attempts to transmit a confidential message to station **B**. The procedure begins when **A** has captured the token and recognized the queued frame(s) to be sent as confidential. Assuming each station maintains a unique IV buffer for every other station capable of confidential communication, **A** would check to see if a valid buffer value exists. If the buffer value is valid, **A** would use the value as the session key K_S for the SECURE_TX procedure. For an invalid IV buffer value, **A** would temporarily store the confidential C_FRAME, then initiate the RESET_KEY procedure.

b. RESET_KEY

RESET_KEY can be initiated by either the receiving or transmitting station. The RESET_KEY procedure must be performed following system initialization, whenever the transmitter/receiver pair session key is not valid, when the session key counter has expired and optionally after an error is detected in a C_FRAME by either station. During

the RESET_KEY operation the basic protocol described for the Central Key Translator is invoked. A key generator is used by the transmitting station **A** to generate an **initialization vector** (IV) value called $\mathbf{IV_{AB}}$. This value is encrypted using the master key $\mathbf{Kt_A}$ shared only by **A** and the **CKT**. Upon receiving the encrypted $\mathbf{IV_{AB}}$ value, the **CKT** decrypts using $\mathbf{Kt_A}$ and then re-encrypts using $\mathbf{Kt_B}$. The translated key is sent to **B** on the same frame. Station **B** uses the master key $\mathbf{Kt_B}$ to decrypt the translated frame from **A**. Station **B** then generates another key value. The new key value is retransmitted in the same frame onto the ring encrypted using the key just received from station **A**. Upon receiving the key frame from **B**, station **A** removes it from the ring.

c. SECURE_TX

The SECURE_TX procedure is used by the transmitting station **A** attempting to transmit C_FRAME(s). Once a valid IV_{AB} is established between the two stations, the station **A** applies the stream cipher function to the C_FRAME. Once it is encrypted **A** transmits the encrypted C_FRAME to **B** using the IV_{AB} as the session key. The encrypted frame(s) travels around the ring passing through all stations connected to the ring until returning to **A**. The recognized C_FRAME(s) are stripped from the medium by **A**. Station **A** then checks the indicator symbols, and compares the frame(s) to the original transmission to ensure the integrity has been maintained. A frame that does not return or is modified suggests a security violation.

d. SECURE_RC

SECURE_RC is the procedure invoked by a receiving station **B** upon recognition of a C_FRAME with a matching destination address. The frame is copied, checked for errors, appropriate frame status field bits set and then retransmitted. If errors were detected B will maintain the last valid IV_{AB} and wait for a retransmital or a RESET_KEY operation followed by retransmital. Assuming no errors are detected B invokes the SECURE_RC procedure. The C_FRAME which was copied into the local

buffer LB_B is decrypted using the stream cipher with IV_{AB} as the session key. If the session key counter has not expired, the IV_{AB} value is maintained, the counter is decremented and the normal FDDI protocol for the receiver resumes control. If the counter has expired a portion of the plaintext INFO field is used as a seed to generate a new session key and the session key counter is reset.

e. GENERATE_KEY

This procedure is used by cryptographic equipped stations to generate new session keys. The procedure may be used as the initial key during a RESET_KEY procedure or when the session key counter has expired to generate a new session key. When used during the RESET_KEY operation the input for the function is generated by a random number generator. When used to change an existing session key the input for the function is part of the plaintext (64 bits) from the previous message.

f. Procedure Notes

{ Denotes optional step }

-- Denotes a comment --

```
Type field is Bit_String
Type FDDI_frame is
    Record
        PA : Preamble_Field;
        SD, ED : Delimeter_Field
        DA, SA : Address_Field;
        RI: Routing_Info_Field;
        INFO : Information_Field;
        FCS : Frame_Check_Sequence_Field;
        FS : Frame_Status_Field;
    end Record;
C_FRAME, K_FRAME,LB_B : Type FDDI_frame;
KEY_SEED, PRG : Type KEY_INPUT;
IV, Kt_A, Kt_B : Type KEY;
A, B, CKT : Type Station;
SESSION_KEY_COUNTER : Type INTEGER;
ENCRYPT, DECRYPT : function STREAM_CIPHER;
```

```
1. RESET_KEY
    Transmitting Station A:
        (IV_AB):= (GENERATE_KEY(PRG));
        K_FRAME.INFO := IV_AB;
        TX to CKT(ENCRYPT((Kt_A( K_FRAME)))); --key is sent CKT under A's masterkey--
    CKT Station :
        RC(ENCRYPT(Kt_A(K_FRAME)));
        DECRYPT (Kt_A( ENCRYPT (Kt_A(K_FRAME)))); --key decrypted using A's master key--
        TX to B: ENCRYPT (Kt_B(K_FRAME); --key re-encrypted and sent under B's master key--
    Receiving Station B:
        RC from CKT(ENCRYPT(Kt_B(K_FRAME));
        (IV_AB):= DECRYPT (Kt_B(ENCRYPT(Kt_B(K_FRAME.INFO));
        K_S := GENERATE_KEY(PRG); --B generates new key--
        TX TO A : ENCRYPT(IV_AB(K_S)); --new session key sent using IV_AB as key--
end Reset_Key;

2. SECURE_TX
    IF C_FRAME queued for TX THEN
            ENCRYPT(({C_FRAME.DA, C_FRAME.SA},C_FRAME. INFO));
            SET FCS (C_FRAME);
            TX to B (C_FRAME);
            IF SESSION_KEY_COUNTER = 0 THEN -- counter expired --
                KEY_SEED:= (1..64(C_FRAME.INFO));
                (IV_AB):= (GENERATE_KEY(KEY_SEED));
                RESET( SESSION_KEY_COUNTER);
            ELSE -- increment counter --
                SESSION_KEY_COUNTER := SESSION_KEY_COUNTER -1;
            END IF;
        end loop;
end SECURE_TX;

3. SECURE_RC is
    IF C_FRAME RX and IV_AB VALID THEN
        CHECK FCS (C_FRAME);
        IF C_FRAME_ERROR THEN
            SET FRAME_STATUS_BITS(ERROR);
            TX to A (C_FRAME);
            MAINTAIN_KEY {RESET_KEY};
            EXIT SECURE_RC;
        END IF;
        LB_B := C_FRAME;
```

```
            SET FRAME_STATUS_BITS(COPIED);
            TX to A (C_FRAME);
            DECRYPT (LB_B );
            IF SESSION_KEY_COUNTER = 0 THEN
                  KEY_SEED:= (1..64(LB_B .INFO));
                  (IV_AB):= (GENERATE_KEY(KEY_SEED));
                  RESET( SESSION_KEY_COUNTER);
            ELSE
                   SESSION_KEY_COUNTER :=  SESSION_KEY_COUNTER -1;
            END IF;
      ELSE IF C_FRAME RX and IV_AB NOT VALID THEN
                  NOTIFY TRANSMITTING STATION  IV_AB NOT VALID
      END IF;
end SECURE_RC;

4. CALL_SETUP
      IF IV_AB VALID THEN
          SECURE_TX(AB);
      ELSE
          RESET_ KEY (AB);
      END IF;
end CALL_SETUP;
```

7. MAC Modifications

Implementation of the proposed confidential communication service at the MAC level would require some modifications to the protocol. These modifications include introduction of some additional variables and procedures which were mentioned in the previous section. In addition, the state transitions within the MAC receiver and MAC transmitter will also require some modification. These modifications entail creating an additional machine state for both the MAC receiver and MAC transmitter. Both of these states represent intermediary points where key establishment and encryption/decryption are facilitated. Aside from these two additional states, the MAC level protocol remains basically intact. The complete receiver and transmitter state transition diagrams as well as abbreviations and algorithms for FDDI MAC-2 are located in Appendix B.

a. MAC Receiver Transitions

Modifications to the receiver state transition machine are required to implement the MAC level security enhancing modification. For MAC receiver modification, a new machine state called RC_SECURE is introduced. This state is an intermediary between RC_FR_CTRL and RC_FR_BODY. There are two possible transition paths between RC_FR_CTRL and RC_SEC_BODY. The first transition occurs when the MAC recognizes the frame as containing a new key which must be decrypted. The second transition occurs when a confidential frame (C_FRAME) is recognized by the flag bit set in the frame control slot. Transition to the RC_FR_BODY occurs after the C_FRAME has been decrypted or a new key is decrypted.

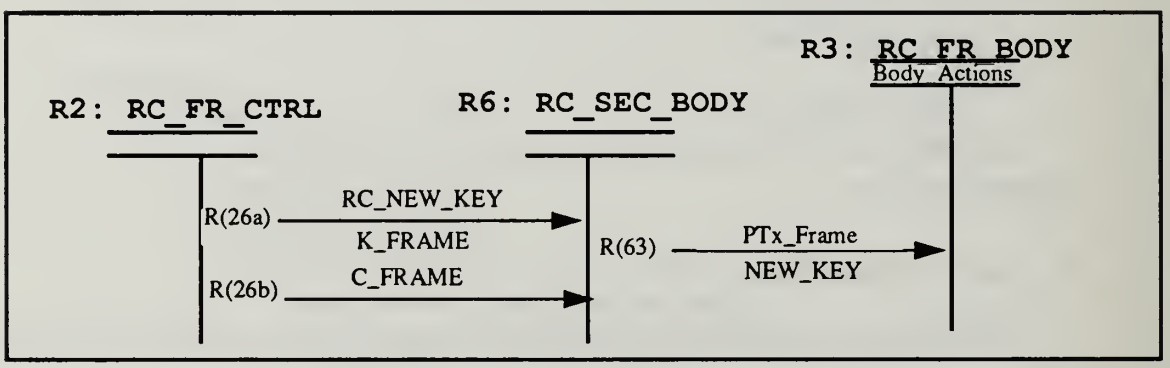

Figure 13. Modified MAC Receiver State Diagram (States Affected)

b. MAC Transmitter Transitions

In order to facilitate the implementation of the confidential communication device, some fundamental modifications to the MAC must be considered. On the transmitter side of the house, an additional machine state is developed. This sixth machine state is called T6: SEC_TX_SETUP and is an intermediary state between the T0: TX_IDLE and T2: TX_DATA states. The purpose of the SEC_TX_SETUP state is ensure all preliminary requirements for a secure transmission are met. Transition to SEC_TX_SETUP occurs from the TX_IDLE state when the next queued frame is flagged

for SECURE_TX (secure transmission). The same conditions apply to the new transition T(06a) that apply to T(02a) with an additional requirement on T(06a) that the frame be designated as confidential. Likewise, the same conditions apply to the new immediate secure transmission transition T(06b) that apply to immediate transmission transition T(02b) with the added confidential designation flag set as in T(06a). A transition T(60) from SEC_TX_SETUP back to TX_IDLE will occur if the Source Address of the of the SEC_TX flagged frame belongs to a station without secure communication capabilities. Transition to the TX_DATA state occurs in one of two ways. First, if a valid key does exist between the SA and DA stations, The frame is encrypted and queued for transmission signalling a transition to TX_DATA. If a valid key does not exist between the SA and DA stations, the frame to be sent is temporarily buffered. A key is generated then encrypted under CKT master key and queued for transmission signalling a transition to TX_DATA. In the case of a key generation, the machine will return to the SEC_TX_SETUP state via T(26) to await arrival of the key.

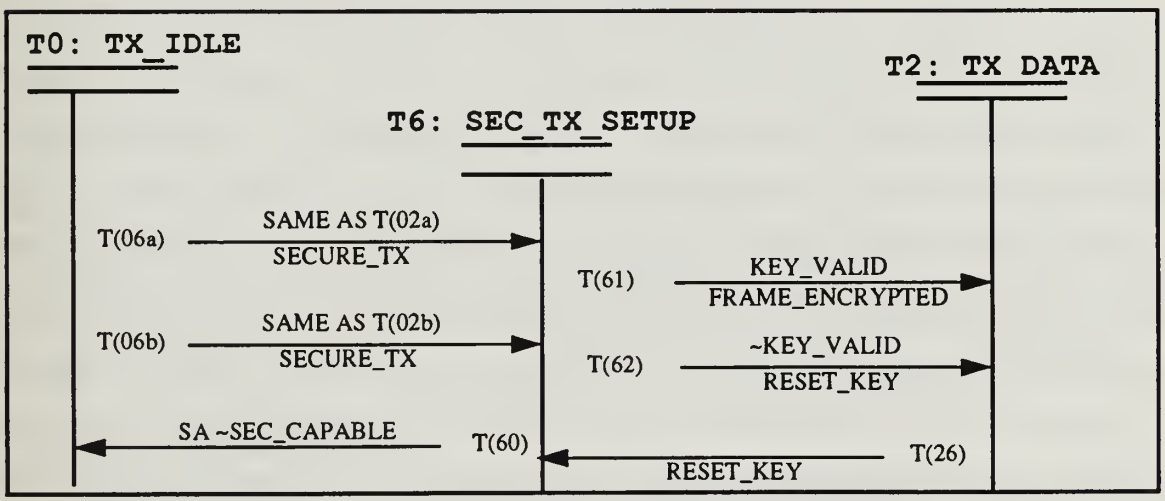

Figure 14. Modified MAC Transmitter State Diagram (States Affected)

8. Degraded Operation Alternatives

One of the attractive features of the dual ring FDDI configuration is the ability to adapt to breaks and defective nodes on the ring. It would seem obvious that some similar

constraints should be imposed upon any mechanism designed to support confidential communication. In other words, what are the implications of losing the CKT node in the previously described design addition? The most obvious alternative would be to continue using the current keys stored in the IV buffers. This would work relatively well assuming valid keys were already established between stations needing confidential communication. However, this an optimal situation and probably not realistic for long periods without the CKT. Several other viable alternatives exist which could be implemented relatively easily.

A simple method to improve the reliability and availability of the system using the CKT would be to include multiple CKT stations. If the primary station becomes inoperable then a secondary station would take over the key translation process. The most effective positioning of a second CKT would be 180 degrees out of phase with the primary translator. This would reduce the likelihood of losing multiple CKTs if a large section of the ring was to fail. However, cost of this redundancy is that fewer operational stations are available.

Although, losing multiple CKT stations simultaneously is less likely, it is possible. Therefore, some other method should be considered for providing some secure communication capability during more serious degraded modes. One possibility is to have a regular station act as a surrogate key translator. This would require that the station maintain valid keys with both of the communicating stations. These would essentially serve the same purpose as the master keys shared between stations and the CKT. A station acting as translator must also be equipped with the logic to perform the rapid decryption/re-encryption process. The same node would not need to act as translator for all station pairs. In fact, only transmitting and receiving stations would be able to determine which stations shared the necessary keys to perform the transaction. In addition, the work load of becoming translator for all stations could greatly inhibit the communication performance of that station.

IV. CONCLUSIONS AND RECOMENDATIONS

A. DISCUSSION

The token ring protocol of FDDI offers a number of security advantages over many other LAN architectures. The principle advantage is that traffic can be regulated by allowing stations to transmit differing amounts of data when controlling the token and by permitting higher priority stations the opportunity to have first claim on a circulating token. The fault management and error checking capabilities provided by FDDI are performed by the MAC monitors at each station to ensure the integrity and availability of message frames. The ability of the ring to shift to a wrapping mode in the event of node failure greatly adds to the survivability and adaptability of the system.

The potential of FDDI for larger LAN and MAN uses is greatly enhanced with a 100 Mbps bandwidth and greater geographical coverage potential. In addition, the media access protocol of FDDI more closely resembles the point-to-point characteristics of wide area networks which typically have different security requirements than local area networks. Currently the IEEE 802 standard for LANs provides an encryption mechanism at the LLC sublayer of the Data Link layer. These mechanisms are more consistent with basic passive contention access protocols than point-to-point systems. Rather than having to rely on a generic LAN security device, a privacy mechanism integrated at the MAC level could more effectively meet the specific high performance needs of FDDI networks. By incorporating a privacy mechanism at the MAC sublayer, we establish a comprehensive security package within the same sublayer which supports the three security elements of *integrity*, *availability* and *confidentiality*.

Within the confines of the design restrictions outlined in Chapter I we have proposed the integration of a MAC level privacy mechanism. The proposed modification should be capable of meeting the high performance demands of current and emerging applications while still maintaining the basic integrity of the FDDI standard protocol. In addition, the

modifications could be implemented using existing commercial encryption standards such as the Data Encryption Standard (DES).

The implementation restrictions stated in Chapter III were determining factors in several of the design decisions. The need for a key server could have been eliminated by using a public key system for key distribution. However, the restriction to employ non-proprietary standards precluded the use of the RSA algorithm. Other public schemes have shown substantial weaknesses or have not undergone the intense scrutiny necessary to instill a high confidence level. Use of a public key distribution scheme as a MAC level privacy mechanism should be explored as a future research project.

The proposal to use a key generating facility at each station would incur considerable cost overhead. A traditional key server system provides only the server with a cryptographic facility. The problem with the conventional server is that the server station has access to all the initial session keys. Using the CKT method does not allow the server access to initial session keys and therefore removes the capability of the server station to access confidential messages. Additionally, the proposed central key translator is more consistent with conventional key server used for the DES.

In terms of overhead, the primary difference between public and private key system storage and access requirements is that public keys may be stored in regular memory, where private keys must be kept in secure (private) memory. The actual memory and access requirements are essentially the same between the two systems. Public key systems use more complex encryption methods which typically makes them slower. However, for key distribution the exponential time overhead may be acceptable.

As mentioned in Chapter I, this proposed security enhancement package is not intended to be an end all solution to replace other LAN security devices in use. The proposed MAC level modifications are intended only as a foundation model for further study and development. Any eventual implementation of a modification such as that proposed must follow an evolutionary path of development. Other issues and concerns not addressed in this thesis will likely influence future design and implementation decisions.

B. FUTURE RESEARCH

The dynamic nature of the information systems industry necessitates ongoing evaluation and updating of security considerations. As new technologies and applications emerge, new security requirements and concerns are raised. This thesis has touched on some of the problems observed in the design and implementation of security enforcing methods. However, many other areas of development remain to be researched. Several possible directions for future research will be discussed.

The effects of incorporating a MAC level security device could be analyzed by modifying an existing FDDI computer simulation or by developing a completly new simulation to validate the assertions made in this thesis, uncover any problems not yet addressed and analyze modified system performance.

As mentioned in this thesis, a MAC level encryption device provides the potential for source and destination address encryption. In order to facilitate an encrypted address scheme, several problems must be addressed. Any encrypted address must not duplicate a plaintext addresses used by any station on ring. In addition, encrypted addresses must not duplicate any ciphertext address currently in use. The problem of duplicate ciphertext address is more complex because these addresses are not static and must not be easily associated with individual stations to be effective. The development of an address encryption scheme would require a complex MAC level address recognition function. Providing this capability would greatly help to deter traffic analysis and add to the overall effectiveness of the security enhancement package.

The restrictions stated in this thesis led to a design decision to use a key server for distributing keys. Several public key distribution protocols could be used for key distribution. If a non-proprietary public key system for session key distribution could be developed and applied to an integrated MAC level security device, the efficiency and security of the protocol could possibly be improved.

Modifications to the FDDI protocol which would significantly improve throughput have been proposed. [Lund 90] These modifications include stripping frames at the receiving station (as opposed to the transmitting station), using both rings for normal operation and allowing sub-tokens to circulate simultaneously. All of these changes affect some aspect of the security in the token ring protocol. For example, stripping frames at the receiving station, will on average deny one half of the ring access to frames either in plain or ciphertext. However, by not allowing the transmitting station to review returning frames some of the integrity and availability capabilities would be adversely affected. Using both rings provides more than one path for data to travel. This means messages could be divided and portions of the message sent along different paths to the same destination. These are only a few of the security implications of surrounding the improved throughput modification. Detailed analysis of where and how these changes will effect the overall security of an increased throughput FDDI would help direct future design modification decisions.

APPENDIX A: FDDI MEDIA ACCESS CONTROL (MAC-2)

A. ABBREVIATIONS

PMD	Physical Layer Medium Dependent
PHY	Physical Layer Protocol
HRC	Hybrid Ring Control
MAC	Media Access Control
SMT	Station Management
CMT	Connection Management Function of Station Management
RMT	Ring Management Function of Station Management
DLL	Data Link Layer
LLC	Logical Link Control
SDU	Service Data Unit
PDU	Protocol Data Unit
PA	Preamble between MAC PDUs
SD	Starting Delimiter
FC	Frame Control field of a MAC PDU
FF	Frame Format bits in Frame Control field of a MAC PDU
DA	Destination Address field of a frame
IG	Individual/Group bit in Destination Address field of a frame
SA	Source Address field of a frame
RII	Routing Information Indicator bit in Source Address field of a frame
RI	Routing Information field of a frame
INFO	Information field of a frame
FCS	Frame Check Sequence field of a frame
ED	Ending Delimiter fieldof MAC PDU
FS	Frame Status field of a frame
E	Error Detected Indicator in Frame Status field of frame
A	Address Recognized Indicator in Frame Status field of frame
C	Frame Copied Indicator in Frame Status field of a frame
MLA	My Long Address
MSA	My Short Address
NSA	Next Station Addressing
Error_ct	Count of reportable frame errors
Frame_ct	Count of all frames received
Late_ct	Count of TRT expirations
Lost_ct	Count of PDUs detected as lost

Not_Copied_ct	Count of PDUs addressed to and not copied by the MAC
Copied_ct	Count of PDUs addressed to and copied by the MAC
Token_ct	Count of tokens received by the MAC
Transmit_ct	Count PDUs transmitted by the MAC
A_Flag	Indicates Destination Address match in last received frame
C_Flag	Indicates successful copying of last received frame
E_Flag	Indicates error detected in last received frame
H_Flag	Indicates Higher Source Address received
L_Flag	Indicates Lower Source Address received
M_Flag	Indicates My Source Address received
N_Flag	Indicates No copy ackknowledgement for this frame
R_Flag	Indicates last valid token received was restricted
D_Flag	Indicates that the duplicate MAC detection delay has transpired
B_Flag	Indicates new restricted dialog may begin on this token rotation
P_Flag	Indicates Purge process
T_Flag	Indicates that the last captured token was early
A_Max	Maximum signal acquisition time
D_Max	Maximum ring latency time
F_Max	Maximum frame time
I_Max	Maximum node physical insertion
L_Max	Maximum transmitter frame set-up time
M_Max	Maximum number of MAC entities allowed on the ring
S_Min	Minimum safety timing allowance
T_Bid_rc	Bidding TTRT received by this MAC in Claim Frames
T_Bid_tx	Bidding TTRT transmitted in this MACs Claim Frames
T_Init	Maximum allowed ring initialization time
T_Max	Maximum TTRT to be supported by this MAC
T_Min	Maximum TTRT to be requested by this MAC
T_Neg	Negotiated TTRT during Claim process (in receiver)
T_Opr	Operative TTRT for this MAC (in transmitter)
T_Pri	Set of n priority Token Rotation Time thresholds
T_Pri[n]	Element n of the set T_Pri
T_React	Maximum allowed time to react to a major ring fault
T_Req	Requested TTRT for this MACs synchronous traffic
T_Resp	Maximum allowed time to recover a token
DM_Min	Minimum duplicate MAC frame detection delay
THT	Token-Holding Timer
TRT	Token-Rotation Timer

TTRT	Target Token Rotation Time
TVX	Valid-Transmission Timer
TVX_value	TVX timeout value

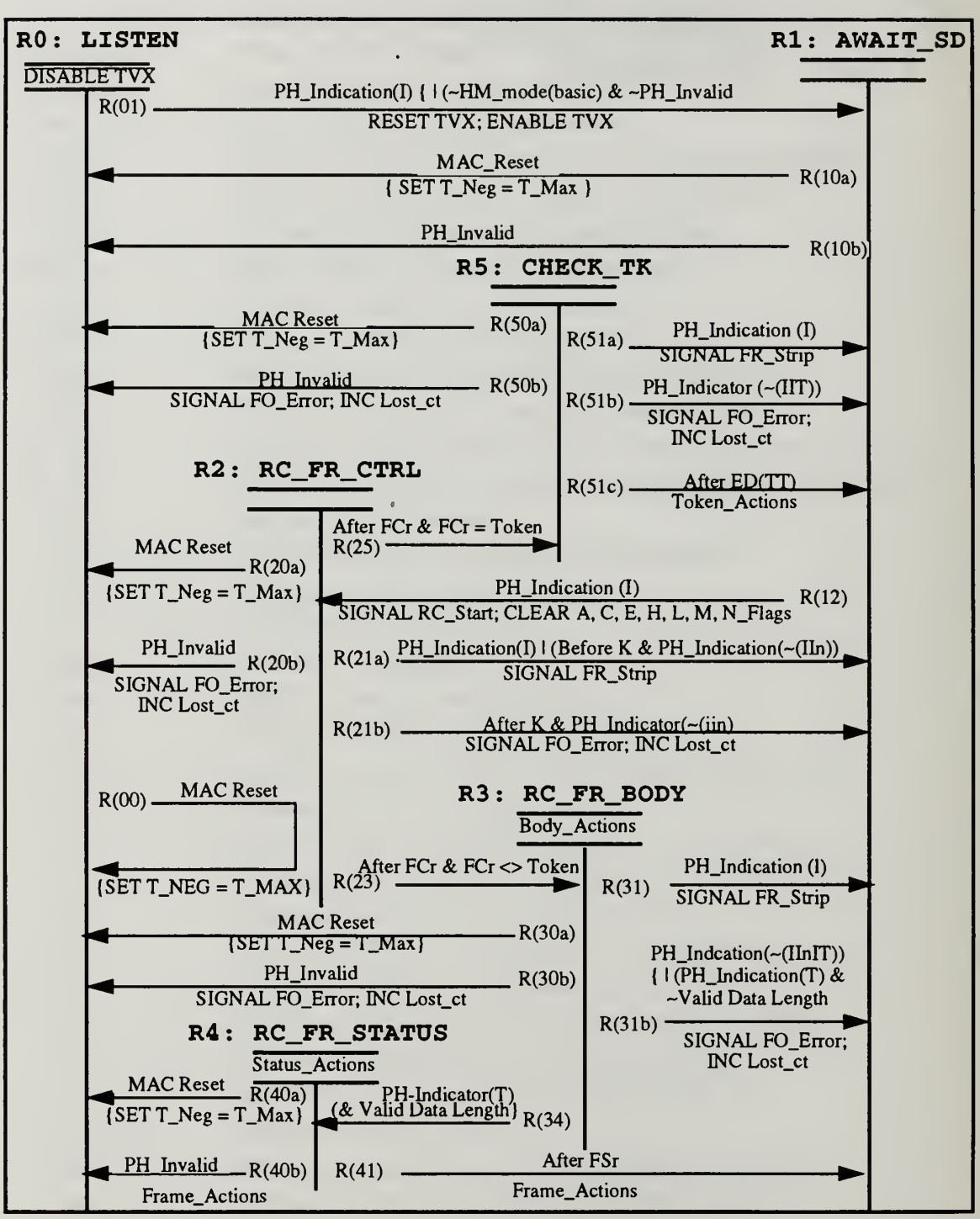

Figure 15. MAC Receiver State Diagram

B. MAC RECEIVER ALGORITHM

```
{ delimits optional term }
--delimits comment--
1. Body_Actions
    After DAr Do
        IF((FCr.L = 0 & DAr element Short_Addresses) |
            (FCr.L =1 & DAr element Long_Addresses))
                Then SET A_Flag;
                    IF FCr <> Void
                        THEN Copy Frame
                        IF FCr = Next Station Addressing
                            THEN SET N_Flag
            { ELSE IF FCr.L = 1 & FCr.FF <> 0 & << transparent bridges >>
                        DAr element Transparent_Bridge_Addrtesses
                        THEN Copy frame; SET N_Flag }
    After SAr DO
        IF (FCr.L = 0 & MSA enabled & SAr = MSA ) |
            (FCr.L = 1 & MLA enabled & SAr =MLA )
                THEN SIGNAL FR_Strip
                    IF SAr > 0
                        THEN SET M_Flag
                ELSE IF SAr > 0
                        THEN IF (FCr.L = 0 & ( MSA disabled | SAr > MSA ) &
                                                ( MLA disabled | MLA = 0 )) |
                                (FCR.L = 1 & (MLA disabled | SAr > MLA ))
                                THEN SET H_Flag
                                ELSE SET L_Flag
    After 4 INFO octets DO
        IF FCr = ( Claim | Purge ) & T_Bid_rc <> T_Req
            THEN IF M_Flag
                    THEN CLEAR A_Flag
                IF T_Bid_rc > T_Req
                    THEN IF L_Flag
                        THEN SET H_Flag; CLEAR L_Flag
                    ELSE IF H_Flag & (( MSA enabled & MSA > 0) |
                                        (MLA enabled & MLA > 0 ))
                        THEN SET L_Flag; CLEAR H_Flag
        IF FCr = Claim &~ H_Flag
            THEN SIGNAL FR_Strip
    { After routing field DO --explicit bridges--
        IF FCr.L = 1 & FCr.FF <> 0 & SAr.RI = 1 &
            Address match in routing field
                THEN SET A_Flag; Copy frame }
```

2. Status_Actions:

```
On entry DO
        INC Frame_ct; SET E_Flag
After Er DO
        IF Er <> RI ' Valid Data Length | ~(Valid FCSr | FCr.FF = Implementor)
            THEN CLEAR A, H, L, M, N_Flags;
                IF FCr = Void & Er = R --for backward compatibility--
                    THEN RESET TVX; CLEAR E_Flag;
            ELSE RESET TVX; CLEAR E_Flag;
                IF ( A_Flag | N_Flag ) & Frame copied
                    THEN SET C_Flag;
                        { IF FCr <> (Void | MAC )
                            THEN INC Copied_ct }
                CASE FCr OF
                    Beacon
                        { SET T_Neg = T_Max; }
                        IF M_Flag
                            THEN SIGNAL My_Beacon
                            ELSE SIGNAL Other_Beacon
                        { Disallow synchronous and restricted requests }
                    Claim;
                        IF H_Flag | ( A_Flag & M_Flag )
                            THEN T_Neg_Actions
                                IF H_Flag
                                        THEN SIGNAL Higher_Claim
                                        ELSE SIGNAL My_Claim
                                ELSE IF ~M_Flag & ((MSA enabled & MSA > 0) |
                                                    (MLA enabled & MLA > 0))
                                        THEN SIGNAL Lower_Claim
                    { Purge: --FDDI-II--
                        IF H_Flag | L_Flag | (A_Flag & M_Flag)
                            THEN T_Neg_Actions;
                                IF A_Flag & M_Flag
                                        THEN SIGNAL My_Purge
                                        ELSE SIGNAL Other_Purge }
                    { Void: --bridge stripping--
                        IF ~ M_Flag
                            THEN SIGNAL Other_Void
                            ELSE IF A_Flag
                                THEN SIGNAL My_Void }
After Ar DO
        IF Ar = R
            THEN CLEAR N_Flag
            ELSE IF Ar = S & A_Flag & DAr.IG = 0 & ~E_Flag &
```

(FCr.FF =) | SAr. RI = 0)
THEN Notify SMT (suspect DA received)

3. Frame_Actions:

IF FCr.C = 1 & FCr.FF = 0 & ~E_Flag
THEN SIGNAL MAC_FRAME; CLEAR R_Flag;
{ disallow retricted requests }
SIGNAL FR_Received;
IF E_Flag & Er <> S
THEN INC Error_ct
{ IF ~ E_Flag & A_Flag & ~ M_Flag & ~N_Flag & ~C_Flag & FCr <> (Void | MAC)
THEN INC Not_Copied_ct }

4. Token_Actions:

IF FCr.L = 1
THEN IF ~R_Flag
THEN SET R_Flag; Notify SMT (restricted token mode)
ELSE RESET TVX; CLEAR R_Flag
{ INC Token_ct } SIGNAL TK_Received

5. T_Neg_Actions:

IF T_Bid_rc < T_Max
THEN SET T_Neg = T_Max;
Notify SMT (invalid T_Bid_rc)
ELSE IF T_bid_rc > T_Min
THEN SET T_Neg = T_Min;
Notify SMT (invalid T_Bid_rc)
ELSE SET T_Neg = TBid_rc

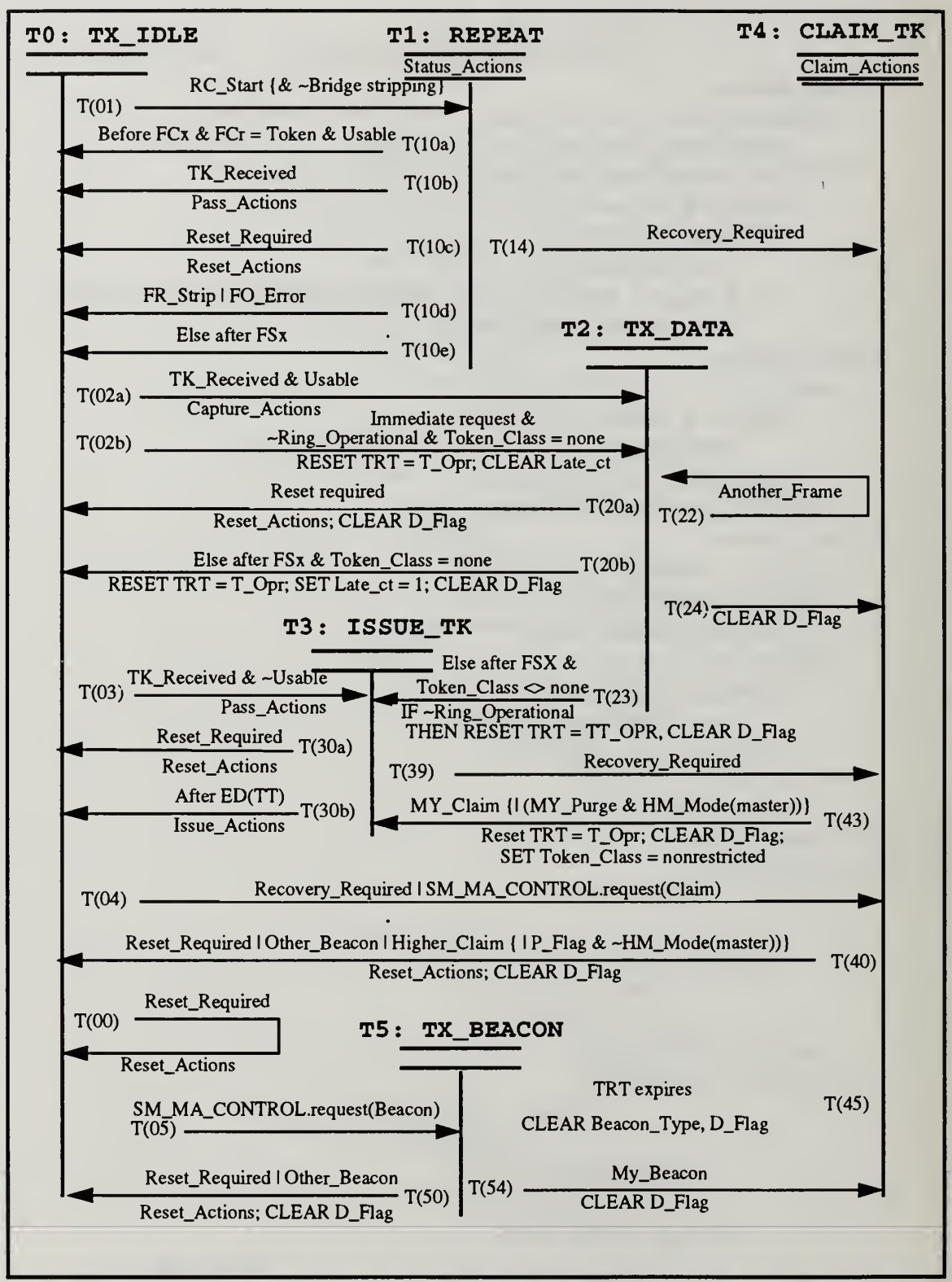

Figure 16. MAC Transmitter State Diagram

C. MAC TRANSMITTER ALGORITHM

```
{ delimits optional term }
--delimits comment--
1. Body_Actions
    Before Rx DO
        IF E_Flag
            THEN SET Ex = S
            ELSE SET Ex = R
    Before Ax DO
        IF A_Flagl Ar = S
            THEN SET Ax = S
            ELSE IF Ar = R
                THEN SET Ax = R
                { ELSE SET Ax = T }
    Before Cx DO
        IF ( C_Flag & ~N_Flag ) I ( Cr = S { & ~A_Flag & Ar <> S ) } )
            THEN SET Cx = S
            ELSE IF Cr = R { I ( A_Flaf & Ar =R ) }
                THEN SET Cx = R
                { ELSE SET Cx = T }
2. Usable_Token
    Ring_Operational &
    ( { ( Synchronous request & Synchronous Allowed ) I }
        ( Asynchronous request & Requested token class = FCr.L &
            Late_ct = 0
            { & (Nonpriority request I TRT < T_Pri[Request priority] ) }
            { & ( Nonrestricted request I
                ( Restricted allowed &
                ( B_Flag I Requested token class = restricted))) } ))
3. Pass_Actions
    IF Ring_Operational
        THEN IF Late_ct = 0
            THEN RESET TRT = T_Opr
            ELSE CLEAR Late_ct
        ELSE SET T_Opr = T_Neg; RESET TRT = T_Opr; SET Late_ct =1;
            SET Ring_Operational
    IF FCr.L = 1
        THEN { CLEAR B_Flag; }
            SET Token_Clas = nonrestricted
        ELSE { SET B_Flag ; }
    { Stop bridge stripping }
4. Capture_Actions:
    DISABLE THT;
```

IF Late_ct = 0
THEN { SET T_Flag; } SET THT = TRT; RESET TRT = T_Opr
ELSE SET THT = expired; CLEAR { T_Flag, } Late_ct
IF FCrL = 1
THEN SET Token_Class = restricted
ELSE SET Token_Class = nonrestricted
{ Stop bridge stripping }

5. Another_Frame:

After FSx & Late_ct = 0 &
({ (~Ring_Operational & Immediate request) | }
(Ring_Operational &
({ (Synchronous request & Synchronous allowed) | }
(Asynchronous request & Requested token class = Token_Class &
(THT unexpired { | (T_Flag & Ignore THT) })
{ & (Nonpriority request | THT < T_Pri[Request priority]) }
{ & (Nonresricted request |
(Restricted allowed &
(B_Flag | Requested token class = restricted))) }))))

6. Issue_Actions:

IF ~Ring_Operational
THEN SET T_Opr = T_Neg; RESET TRT = T_Opr; SET Late_ct =1
{ ELSE IF Token_Class = nonrestricted & ~R-Flag
THEN SET B_Flag
ELSE CLEAR B_Flag }

7. Reset_Required

MAC_Reset | SM_MA CONTROL.request (send_mac_frame) |
(MAC_Frame &
(Ring_Operational | Late_ct = 0 |
(Token_Class <> none & ~My_Claim { & ~My_Purge })))

8. Reset_Actions:

SET T_Opr = T_Max; RESET TRT = T_Opr; SET Token_Class = none;
IF MAC_Reset
THEN CLEAR Late_ct, Ring_operational, D_Flag
ELSE IF Ring_Operational | Late_ct =0
THEN SET Late_ct =1; CLEAR Ring_Operational
{ CLEAR B_Flag; Stop bridge stripping }

9. Recovery_Required:

(TVX expired { & ~HM_mode(slave) }) |
(TRT expires & Late_ct > 0
{ & (~ HM_mode(slave) | (~Ring_Operational & Token_Class = none)) }) |
{ (HM_mode(master) & ~Ring_Operational & Token_Class = none) | }
Lower_Claim

10. Claim_Actions:

```
On entry DO
    SET T_Opr = T_Max: RESET TRT = T_Opr; SET Token_Class = none;
    IF Ring_Operational | Late_ct = 1; CLEAR Ring_Operational
        { CLEAR B_Flag; Stop bridge stripping }
    { CLEAR P_Flag;
    IF SM_MA_CONTROL.request(Claim)
        THEN HP_MODE.request(HP_Mode(basic)) }
REPEAT
    { IF HM_mode(master)
        THEN HP_MODE.request(HP_Mode(any)); SET P_Flag;
            Transmit Purge Frame
        ELSE HP_Mode.request(HP_Mode(basic)); }
            Transmit Claim Frame
Before T_Bid_tx DO
    SET T_Bid_tx = T_Req
```

11. TRT Actions:

```
Always DO
    IF TRT > T_Opr + DM_Min & ~Ring_Operational & ~D_Flag
        THEN SET D_Flag
    IF TRT expires
        THEN
            { IF LATE_CT > 0 & HM_Mode(slave) &
                ( Ring_Operational | Token_Class <> none ))
                THEN SET T_Opr = T_Max;
                    RESET TRT = T_Opr;
                    SET Token_Class = none; CLEAR Ring_Operational;
                    CLEAR B_Flag; Stop bridge stripping
                ELSE }
                    RESET TRT = T_Opr
                    IF Late_ct < 255
                    THEN INC Late_ct
```

APPENDIX B: DATA ENCRYPTION AND NETWORKS

A. OVERVIEW OF CRYPTOGRAPHY

Traditionally, security in computer networks has been facilitated through data encryption/decryption.[6] Advances in breaking ciphers coupled with faster more advanced computers to employ these methods, raise questions about the ability of traditional cryptographic techniques to provide a high degree of security. Furthermore, in order to make these techniques more trusted they often become more complex. As cryptanalysis becomes more sophisticated so must encryption techniques. This often leads to slower less reliable systems which may be unacceptable in a real time environment requiring high data rates rapid response times. Several standards for data encryption are in use with the Data Encryption Standard (DES) probably being best known.

Encryption is a process of encoding a message so that the meaning is not readily apparent to an unintended observer; *decryption* is the process of transforming the original message back into original form. The original message is called *plaintext* while the encrypted message is referred to as *cipher text.*

***Ciphertext*: C = E(P)**
***Plaintext*: P = D(C)**

We will denote plaintext as **P** and ciphertext as **C.** The transformation between plaintext and ciphertext is accomplished using some encryption function denoted as **E**, and a reverse decryption function **D**. Many algorithms employ a key **K** with the ciphertext dependent on both the original plaintext message and the key value.

In general, certain principles should be considered when choosing a cipher for a specific application. The overhead associated with encryption and decryption should be consistent with the level of security necessary. The enciphering algorithm and key

management technique should be free from complexity. [Shan 49] However, the algorithm need not be simple as long as the time complexity is tolerable for the application. Errors in ciphering should not propagate and cause further corruption of the message. The size of the ciphertext message should never exceed the original plaintext message.

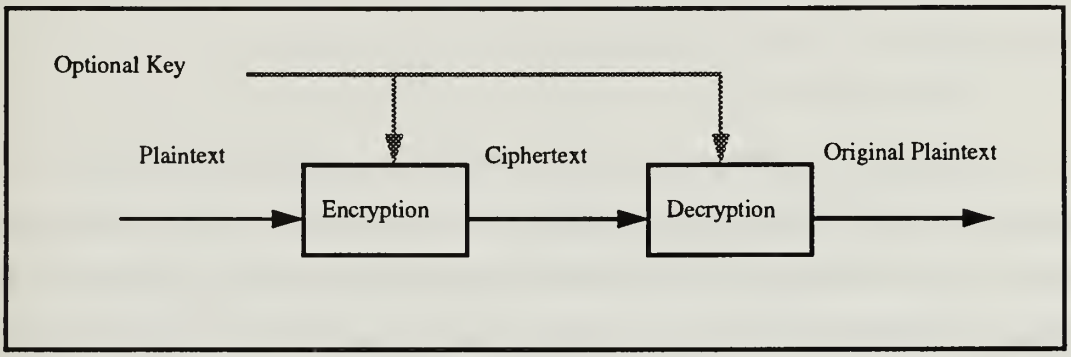

Figure 17. Basic Crypto System

Some encryption techniques use a key **K**, which determines the ciphertext. Data is still considered protected with a public algorithm as long as the key is secret. However, keys are generally shorter than the plaintext to be encrypted and thus are more susceptible to cryptanalysis given enough ciphertext to analyze.

A session key is designed to be changed after a prescribed time has passed or certain amount of data has been transmitted. By changing keys periodically, an intruder has more difficulty accumulating enough data to determine the key. Even if the key is discovered it will be changed again when the session has expired. The biggest problem with session keys is providing an efficient and secure method of distribution.

A network *key server* is a process that distributes keys to users on request. The key server shares a unique key with each station. If station **A** wants to communicate with station **B**, **A** must call the key server saying a session key is desired between stations **A** and **B**. The key server then generates a new key which it sends to **A** and **B**. **A** and **B** both decrypt the session key $\mathbf{K_S}$, and transact their session using $\mathbf{K_S}$. This method can be used to provide end-to-end encryption without the massive number of keys normally needed. Each station

requires only a single key to communicate with the key server. The amount of ciphertext between the central key server and each station is small enough o make cryptanalysis of the master keys difficult. The unique key shared between each station and key server facilitates peer to peer authentication between stations **A** and **B**.

1. Stream Ciphers

The basic bit stream cipher used for network encryption is a form of substitution. This method usually incorporates a cipher key which is used as a seed to a pseudo-random number generator (PRG). The output bit stream from the PRG is referred to as the **Initialization Vector** (IV) and is combined by modulo 2 addition with plaintext to produce the ciphertext. A similar approach is the bit stream cipher with cipher feedback where ciphertext is returned to the PRG as a parameter. A third technique is to use plaintext as feedback to the PRG. A variation of the previous techniques would be to delete the PRG and use a continuous random bitstream key. This method provides a theoretically unbreakable one time cipher, provided the key stream is used only once. This means given a plaintext message, it would never be encrypted the same way twice. [Muft 91]

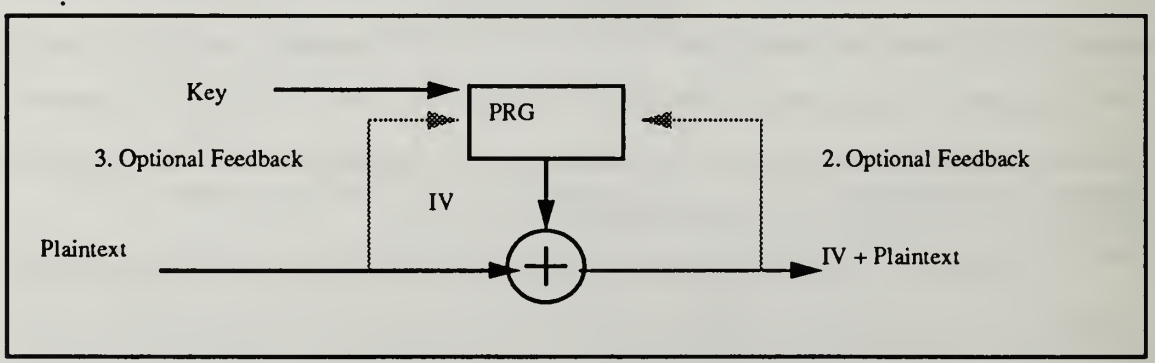

Figure 18. Stream Cipher Variations

The simple bit stream cipher is easy to perform and does not require a complicated algorithm for decryption. The complexity of the cipher corresponds to direct translation with an order of magnitude of ***n***. In bit stream ciphers, individual symbols are encrypted

independent of the original plaintext symbols. This means that the only way to build a reversible crypto function is through modulo two addition. In terms of complexity, the speed to transform the plaintext into ciphertext is only dependent on the algorithm itself and not the time it takes to receive more plaintext. Errors are not propagated because each symbol is encrypted as a separate entity, and a single error in the encoding process will cause an error in only a single character. With no error propagation it is often possible for the receiving station to determine the correct character in error.

Bitwise enciphering does expose several disadvantages. A cryptanalyst could more easily analyze the characteristics of individual symbols in the ciphertext and attempt to break the encryption using digram analysis, distribution counts, index of coincidence or several other tools. Once a code is broken a malicious intruder could destroy the integrity of passing messages by splicing together pieces of previous messages and transmitting a spurious new message which may look authentic.

2. Block Ciphers

The second basic method of encryption called a block cipher is based on transposing the message across the cipher text. The purpose of the transposition is to diffuse the message by breaking up established patterns. A simple block cipher might involve transposing columns into rows. The plaintext columns are divided into blocks of a defined length and then reassembled by arranging the blocks into rows. Cryptanalysis methods for block ciphers are not as scientific as for substitution ciphers. This is particularity true when multiple transpositions have been performed. The cryptanalyst is forced to make more "guesses" at probable plaintext to obtain clues about the transposition. It is often necessary to perform a letter frequency distribution to determine if a block cipher has even been applied. Attacks on block ciphers are usually based on common letter pairs and triplets called digrams and trigrams, which appear frequently in plaintext. A cryptanalyst may use the knowledge of these patterns to match plaintext characters which have been separated in the transposition. Once the plaintext and ciphertext character position relationship is

determined, the algorithm is basically broken. Another distinct disadvantage of transposition ciphers is that the message cannot be decrypted until all of the message is read. Although the time complexity of the algorithm is proportional to the length of the message, so is the delay associated with reading the entire message before beginning deciphering. These algorithms also incur added storage requirements. These considerations make transposition algorithms less appropriate for long messages or when a rapid response time is required. [Carr 90]

3. Key Systems

a. Conventional Key Encryption

Conventional key encryptions systems are based on the sharing of a single secret key by all authorized parties. This type of key system utilizes the same key for both the encryption and decryption functions. Consequently, communicating stations can each send and receive messages using the same key. For this reason conventional secret key systems are referred to as symmetric.

Messages encrypted using a conventional key system are inherently authenticated provided that the secrecy of the key is trusted. In other words an encrypted message transmitted by **A** using **A** 's key must have been transmitted by **A** since only **A** has access to the key. One problem is that if each transmitting/receiving station pair is to share a unique key, then the total number of keys required increases with the square of the number of stations requiring keys.

Keys must be distributed in a secure manner since they allow access to all information encrypted under them. One approach to the distribution problem is to use a key server that distributes keys to users on request. The key server shares a unique master key with each station. When two stations wish to communicate confidentially the server delivers a session key to each station encrypted under their respective master keys. Figure 17. depicts the protocol for central key server operation. By using a key server, each station only needs to maintain a single master key with the server and the session key in use.

However, establishing new session keys with every new communication may incur an unacceptable overhead for applications which require rapid response times. Numerous keys being distributed could also occupy considerable bandwidth resulting in less efficient system performance.

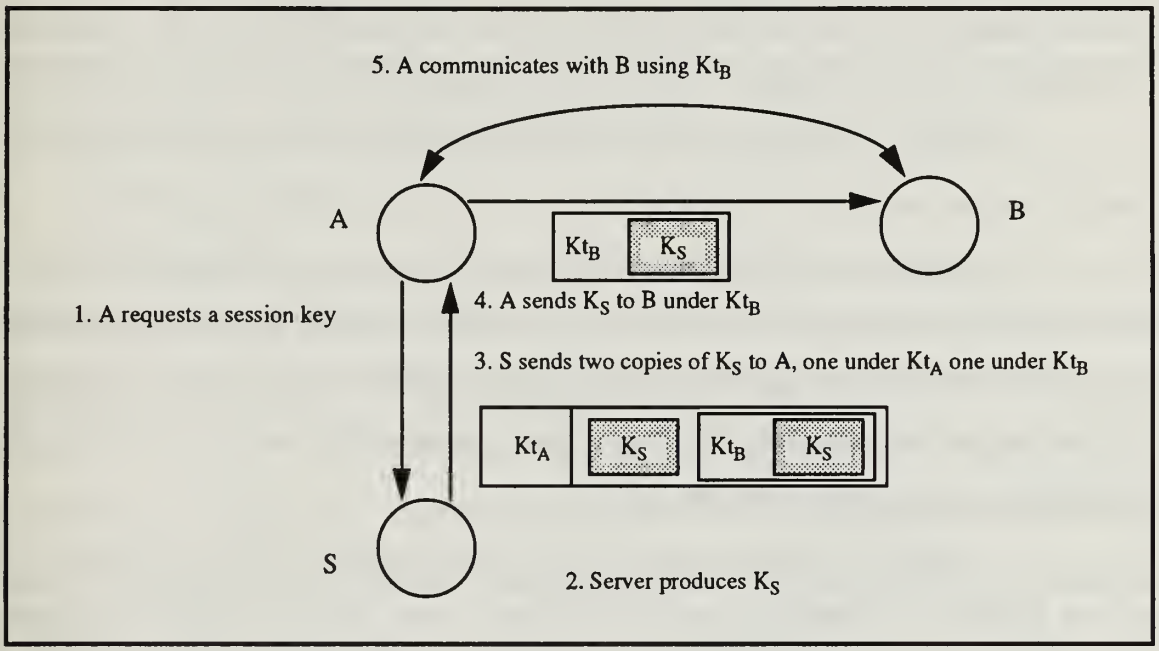

Figure 19. Key Server Distributing Session Keys

b. Public Key Systems

Public key systems are based on the principle of providing each user with two keys: a private key and a public key. The two keys operate as inverses with the public key used to perform a one way encryption and the secret key used to decrypt. In other words a user can decrypt a message using a private key that someone else encrypted using the corresponding public key. An additional property is that the two keys can be applied in either order.

$$P = D(k_{private}, E(k_{public}, P))$$

or

$$P = D(k_{public}, E(k_{private}, P))$$

With public keys, only two keys are needed per user for communication capability with all other stations. However, peer-to-peer authentication is not inherent since every station may have access to all public keys. Authentication can be provided in a public key system using a double encryption. [Need 78] A message encrypted by transmitting station **A** using **A**'s private key then encrypted again using receiving station **B**'s public key, will be both secret and authentic. Authenticity is provided by A's private key which only A can use to encrypt. Likewise secrecy is provided by B's public key which only B can decrypt with the secret key.

Public key systems are typically based on much more complex problems than single key systems. This complexity usually translates to slower encryption/ decryption speeds. Slower speeds coupled with the requirement for double encryption to support peer-to-peer authentication and privacy make public keys less attractive for applications requiring rapid response times.

With the exception of the Rivest-Shamir-Adelman (RSA) encryption, most of the public key algorithms seen to date have been shown to exhibit substantial weaknesses. A number of public key encryption schemes have recently been introduced but have not been in existence long enough to have undergone the intense scrutiny by cryptanalysis professionals needed to instill a high confidence level.

Public systems require each station to maintain a private and a public key. However, for one stations to use another stations public key, it must either store the key or request the key from another station. The primary difference between public and private key system storage and access requirements is that public keys may be stored in public memory, where private keys must be kept secret. The actual space and time requirements are essentially the same.

B. DATA ENCRYPTION STANDARD (DES)

The Data Encryption Standard (DES) is a product cipher which was developed by IBM. The encryption algorithm has since been implemented in hardware making it fast and cheap. In contrast to earlier cryptographic techniques with long keys, the DES relies on a 56 bit key with a 19 stage complex convoluted algorithm using both transposition and substitution. The DES is capable of operating in a block as well as bit stream cipher mode. The block mode is subject to the limits discussed and is not used in our method.

C. RIVEST-SHAMIR-ADELMAN (RSA) ENCRYPTION

The RSA algorithm is based on the hard problem of determining the prime factors of a large target number. Unlike the public key system described previously, RSA does not distinguish between public and private keys. The encryption and decryption keys are referred to as *e* and *d* respectively. The encryption algorithm uses exponentiation performed mod *n* against the plaintext block (P^e mod n). This makes it very difficult to factor P^e and discover the plaintext. The decrypting key is chosen such that $(P^e)^d$ mod n = P. Therefore, the decryption does not require P^e to be factored.

$$\mathbf{Ciphertext = Plaintext^e \bmod n}$$

$$\mathbf{Plaintext = Ciphertext^d \bmod n}$$

Despite extensive study by cryptanalysts, no serious flaws have been discovered in the RSA algorithm. However, the fastest known algorithm for the RSA factorization is exponential in time. In addition, the public key nature of RSA necessitates a double encryption to provide peer-to-peer authentication. Although the RSA is available in hardware, the complexity of the algorithm limits the usefulness for real time applications. The RSA is also a patented device.

D. LINK VS. END TO END ENCRYPTION

Encryption in networks is applied either between two hosts or between two applications. These two methods are called link encryption and end-to-end encryption. With link encryption data is encrypted at layers 1 or 2 in the OSI model just prior to being placed on the physical medium. The message is protected as it passes between two nodes but is actually decrypted and then re-encrypted at each host. In other words, the message is in plain text inside the host. Link encryption is especially vulnerable when messages must pass through one or more additional hosts between sender and receiver. End-to-end encryption security is provided from the transmitting station to the receiving station. As the message passes through each node it remains encrypted. End-to end encryption is usually performed at levels 6 or 7 of the OSI model. [Voyd 85]

LIST OF REFERENCES

[Adam 92] Adam, J.A., "Data Security," *IEEE Spectrum*, August 1992, pp. 19-44.

[Carr 90] Carrol, John M., "Do-it-Yourself Cryptography," *Computers and Security*, September 1990, pp. 613-619.

[Coom 91] Coomaraswamy, G., Kumar, S.P. and Marhic, M.E., "Fiber-Optic LAN/ MAN Systems to Support Confidential Communication," *Computers and Security*, v. 10, 1991, pp. 756-776.

[Ehrs 78] Ehrsam, W. "A Cryptographic Key Management Scheme for Implementing the Data Encryption Standard." *IBM Systems Journal*, v. 17, no. 2, 1978, pp. 56-61.

[FDDI 87] FDDI Token Ring Media Access Control (MAC), ANSI Standard X#.139-1987, REV 10.

[FDDI 91] FDDI Media Access Control (MAC II), Rev 4.0, 1990.

[Hall 91] Halloran, F. and others, "An FDDI Network for Tactical Applications," *IEEE LCS*, February 1991, pp. 29-35.

[Koch 91] Kochanski, R. J., Paige, J.L., "SAFENET: Standard and its Application," *IEEE LCS*, February 1991, pp. 46-51.

[Lund 90] Lundy, G.M., "Improving Throughput in the FDDI Token Ring Network," Naval Postgraduate School 1990.

[Muft 91] Muftic, S., *Security Mechanisms For Computer Networks* West Sussex, England 1989.

[Need 78] Needham, R.M. and Schroeder, M.D., "Using Encryption for Authentication in Large Networks of Computers," Communications of the ACM, vol. 21, no. 12, pp. 993-999, December 1978.

[Pfle 89] Pfleeger, C. P., *Security In Computing*, Prentice Hall Inc., New Jersey, 1989.

[Ross 89] Ross, F. E., "An Overview of FDDI: The Fiber Distributed Data Interface," *IEEE Journal on Selected Areas in Communications*, September 1989.

[Schn 85] Schnackenberg, D.D., Development of a Multilevel Secure Local Area Network, *Proceedings of the 8th National Computer Security Conference*, 1985, pp. 97-104.

[Shan 49] Shannon, C. "Communication Theory of Secrecy Systems," *Bell Systems Technical Journal*, v. 28 October, 1949, pp. 656-715.

[Stal 91] Stallings, W., *Data and Computer Communications*, 3d. ed., Macmillan Publishing Company, 1991.

[Tard 85] Tardo, J., "Standardizing Cryptographic Services at OSI Higher Layers," *IEEE Communcations Magazine*, July 1985, pp. 25-29.

[Voyd 85] Voydock, V., Kent, S.,"Security in High-Level Network Protocols", *IEEE Communications Magazine.*, July 1985, pp. 12-24.

[Stoll 90] Stoll, C., *The Cuckoo's Egg*, POCKET BOOKS, New York 1990.

BIBLIOGRAPHY

Abrams, M.D., Podell, H.J., *Tutorial Computer and Network Security*, IEEE Computer Society Press, 1987.

Chorafas, D. N., *Handbook of Data Communications and Computer Networks*, TAB BOOKS, 1991.

Coomaraswamy, G., Kumar, S.P.R. and Marhic, M.E., "Fiber-Optic Configurations Supporting Confidentiality in Passive DQDB Systems," *Proceedings IEEE INFOCOM '91*, v. 2, April, 1991, pp. 901-910.

Hoffman, L.J., *Modern Methods for Security and Privacy*, Prentice Hall, 1977.

Johnson, D.B., and others, "Common Cryptographic Architecture Cryptographic Application Programming Interface," *IBM Systems Journal*, v. 30, no. 2, 1991.

Keck, D.B. "Fundamentals of Optical Waveguide Fibers," *IEEE Communications Magazine*, v. 23, no. 5, May 1985.

Lundy, G.M., Akyildz, I.F., "Specification and Analysis of the FDDI MAC Protocol Using Systems of Communicating Machines," Naval Postgraduate School, Monterey, CA., September 6, 1991.

Marhic, M.E., Chang, Y.L., "Pulse Coding and Coherent Decoding in Fibre-Optic Ladder Networks," *Electronics Letters*, v. 25, no. 22, October 26, 1989.

Matyas, S.M., Le, A.V. and Abraham, D.G., "A Key Management Scheme Based on Control Vectors," *IBM Systems Journal*, v. 30, no. 2

Muftic, S., "Transaction Protection by Antennas," *Computers and Security*, September, 1990, pp. 245-255.

Preneel, B., and others, "Cryptanalysis of a Fast Cryptographic Checksum Algorithm," *Computers and Security*, September, 1990, pp. 257-261.

Schoemaker, S., *Computer Networks and Simulation III*, Elsevier Science Publishers, 1986.

Tannenbaum, A. S., *Computer Networks*, 2d ed., Prentice Hall, 1988.

Tassel, D.V., "Computer Network Cryptography Engineering," *National Computer Conference Information Technology Series*, v. 3, AFIPS PRESS, 1978, pp. 197-202.

U.S. Department of Commerce, National Bureau of Standards, *Design Alternatives for Computer Network Security*, Government Printing Office, Washington D.C., 1978.

INITIAL DISTRIBUTION LIST

1.	Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
2.	Dudley Knox Library Code 52 Naval Postgraduate School Monterey, CA 93943-5002	2
3.	Chairman, Code CS Code CS, Department of Computer Science Naval Postgraduate School Monterey, CA 93943-5100	2
4.	Dr. G.M. Lundy Code CS/Ln, Department of Computer Science Naval Postgraduate School Monterey, CA 93943-5100	1
5.	Roger Stemp Code CS/Sp, Department of Computer Science Naval Postgraduate School Monterey, CA 93943-5100	1
6.	Lieutenant Benjamin E. Jones 7788 Alspice Circle East Jacksonville, FL 32244	1
7.	Curricular Office Code 37, Department of Computer Science Naval Postgraduate School Monterey, CA 93943-5100	1
8.	Commander Naval Computer and Telcommunications Command 4401 Massachusetts Ave., N.W. Washington, D.C. 20370-5000	1
9.	CDR Debbie Campbell National Computer Security Center NSA / C81 / APSXI 9800 Savage Rd., Ft. Meade, MD 20755-6000	1
10.	Naval Information Systems Managenment Center Building 166, Washington, D.C. 20374-5070	1

11. SPAWAR 1
Code 2241
Crystal City 5CPK, 700
Washington, D.C. 20363-5100